NetIQ® AppManager® Knowledge Script® Reference Guide

October 2011



Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 2011 NetIQ Corporation, all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

Contents

About this Book and the Library lv
About NetIQ Corporation lvii

Chapter 1
Introduction to Knowledge Scripts **1**
Introduction to Knowledge Script Categories 1
Understanding Resource Types and Type Checking 1
Understanding How Knowledge Scripts Work 2
Setting Knowledge Script Properties 4
Viewing Job Results 5
Viewing Detailed Information 5
Using Filters to Fine-Tune Searches 6
Running Knowledge Scripts that Require Special Privileges 9
Getting Online Help for Knowledge Scripts 10

Chapter 2
Action Knowledge Scripts **11**
AddComputerToServerGroup 13
Diagnose 14
DiagnoseNortelIPT 16
DiagnoseVoIPQuality 18
DominoCommand 20
DosCommand 21
DumpTran 23
ExtendedSNMPTrap 24
IISContinueSite 25
IISPauseSite 26
IISRestartServer 27
IISRestartSite 28
MapiMail 29
Messenger 32
NetAppFilerDoSnapMirror 35
NetAppFilerIssueCommand 36
NetAppFilerReboot 37
NotesMail 38
NTEventLog 41
Page 44
RebootSystem 48
RestartServices 49
RunDiscoveryCiscoCallMgr 50
RunDiscoveryNetworkDevice 52
RunKS 54
RunPhoneInventory 58
RunPowerShell 60
RunSql 62

SendReportToPrinter 63
SMTPMail 65
SMTPMailRpt 68
SNMPTrap 71
StartServices 74
StopServices 75
Traceroute 77
TracerouteNetworks-RT 79
UpdateEventStatus 80
UXCommand 81
WriteMsgToFile 82

Chapter 3
AD Knowledge Scripts **85**
AD Knowledge Script Job Delegation 88
Authentications 89
BridgeheadChange 91
CacheHitRate 93
ClientSessions 95
ConnectivityObject 97
DatabaseSize 98
DCAdvertised 100
DCHealthMonitor 101
DCInSiteConnectivity 104
DomainConnectivity 106
EnumerateSites 108
EventLog 110
EventLog (NetLogon) 113
EventLog (W32Time) 116
FSMOChange 119
FSMOHealth 121
FSMOPlacement 123
GlobalCatalogChange 125
GlobalCatalogHealth 127
InboundReplStat 129
InterReplTraffic 131
IntraReplTraffic 133
KCCConnections 135
KCCDisabled 136
KDCRequests 138
NumberOfComputers 140
NumberOfDCs 142
NumberOfGCs 144
NumberOfGroups 146
NumberOfObjects 148
NumberOfPrintQueues 150
NumberOfUsers 151
NumberOfUsersLocked 153
OutboundReplStat 155
PropertyWatch 156
ReadStat 158

ReplEventLog....160
ReplicationCheckByUSN....163
ReplicationLatency....164
ReplQueueLen....169
ReplSysVol....171
ReportADSI_ADObjects....173
ReportADSI_GroupMembership....175
ReportADSI_LocalService....177
ReportADSI_LocalUser....179
ReportADSI_ReplicationLatency....181
ReportADSI_ReplSysVol....183
ReportADSI_ServerRoles....185
ReportADSI_UserAccountsDisabled....187
ReportADSI_UserBadPasswordCount....189
ReportADSI_UserMemberOfMoreThanOneGroup....191
ReportADSI_UserPasswordExpired....193
ResponseTime....195
SearchStat....197
ServerHealth....199
SyncRequest....202
WriteStat....204
AD Knowledge Script Groups....206
AD....207
AD (all DCs)....209
AD (one DC per domain)....210
AD (one DC per forest)....211
AD (one DC per site)....212

Chapter 4
AD-RT Knowledge Scripts 213
CheckDomainController....214
DNSNameLookup....216
DNSSpecificServerNameLookup....218
GetObject....220
QueryService....223
Report_AD-RT....226
Report_AD-RT_DNS....228

Chapter 5
AMAdmin Knowledge Scripts 231
AgentConfigMSRestrictions....233
AgentConfigSecurityKey....237
AgentConfigSecurityLevel....239
AgentHealth....241
AgentSelfMon....243
ChangeFooter....245
ConcurrentRpt....246
ConfigAdminEvents....247
ConfigSiteCommType....250
ConfigSiteNetFlowCtrl....251

DBHealth 253
DeleteExpiredReports 257
DisableSiteComm 258
EnableSiteComm 261
GreyMachines 264
IISContinueSite 266
IISPauseSite 267
IISRestartServer 268
IISRestartSite 269
LRReadParameters 270
LRRemoveParameters 272
LRWriteParameters 274
MonitorMSCommunications 276
MSHealth 277
RemovePrimaryMS 279
SchedMaint 280
SetAllowMS 282
SetDataTimeStamp 284
SetDeploymentWebService 286
SetKSStandby 287
SetLocalRPSize 288
SetPrimaryMS 289
SetReportPaths 292
SetResDependency 294
SiteSchedUpload 296
UpgradeJobs 298

Chapter 6
AMAdminUNIX Knowledge Scripts 307
AgentHealthProxy 308
AgentInstallProxy 312
AgentUpdate 325
AgentUpdateSecurityLevel 327
SchedMaint 329
SetPrimaryMS 331

Chapter 7
AM Health Knowledge Scripts 335
CCComponentsHealth 336
HeartbeatUNIX 341
HeartbeatWin 343
QDBComponentsHealth 346
Recommended Knowledge Script Groups 351

Chapter 8
Apache UNIX Knowledge Scripts 353
AccessActivity 355
AccessLogEntries 357
Availability 358
ConfigFileUpdateCheck 359

ConfigTest 360
CoreDumpCheck 361
CPU 362
ErrorLogEntries 363
HealthCheck 364
InfoModule 366
KillLongRunningRequests 367
KillProcessesAboveCPU 368
ModuleEnabled 369
ProcessActivity 370
Report_ActivitySummary 371
Report_HealthSummary 374
Report_PerformanceSummary 377
Requests 379
ServerUtilization 381
StartServer 383
StatusModule 384
StopServer 385
Throughput 386
TopNPageActivity 388
Uptime 389
VirtualMemory 390
Discovery_ApacheUNIX 391

Chapter 9
Application Knowledge Scripts **393**
ApplicationDown 394
CpuHigh 395
MemoryHigh 396

Chapter 10
ARCserve Knowledge Scripts **397**
ActivityLogSize 399
AlertMediaChange 400
CanceledJobs 401
DeleteJobs 402
EventLog 403
FailedJobs 405
HungJobs 406
IncompleteJobs 408
LogFiles 410
Report_ActivityLogSize 411
Report_CPUandMemoryUsage 414
Report_NumberofCanceledJobs 417
Report_NumberofFailedJobs 420
Report_NumberofIncompleteJobs 423
Report_NumberofSuccessfulJobs 426
RescheduleJobs 429
ResourceHigh 430
ServiceDown 431

SetLoggingType 432
SuccessfulJobs 433

Chapter 11
ASYNC Knowledge Scripts **435**
Creating Filters with Regular Expressions 436
FilesChanged 438
NTEventLog 439
NTEventLogRx 442
SNMPTrap 446

Chapter 12
AvayaCM Knowledge Scripts **455**
AddMIB 457
AddPhone 459
Announcements 461
AttendantCalls 464
CallActivity 467
CallFailures 469
CallQuality 473
CallQuery 478
CPU_Usage 481
ESS_Status 483
H248GatewayStatus 484
HuntGroupUsage 486
LSP_Status 488
PhoneConnectivity 489
PhoneDeregistrations 491
PhoneInventory 493
PhoneQuality 495
RegisteredResources 499
RemovePhone 503
RetrieveConfigData 504
SecurityViolations 506
SetupSupplementalDB 509
SNMPTrap 512
SystemUptime 518
TrunkGroupUsage 519
Recommended Knowledge Script Group 522

Chapter 13
BackupExec Knowledge Scripts **523**
AbortedJobs 525
ActiveJobIDs 526
CompletedJobs 527
FailedJobs 528
IncompleteJobs 529
LatestJob 530
Report_Availability 531
Report_IDsofActiveJobs 533

Report_NumberofAbortedJobs 536
Report_NumberofCompletedJobs 539
Report_NumberofFailedJobs 542
Report_NumberofIncompleteJobs 545
Report_StatusofTheLatestJob 548
ResourceHigh 551
ResubmitFailedJobs 552
ServiceDown 553
SkippedFilesInJobs 554
SuccessfulJobs 556
TotalBytes 557

Chapter 14
BES Knowledge Scripts **559**
BlackberryAgent 561
DebugLogSearch 564
DebugLogSize 568
HungThreads 570
InactiveUsers 575
MDSConnections 577
MDSFailures 581
MessageSize 584
OrphanedUsers 586
Report_EndToEndResponseTime 588
Report_LastUserCount 590
Report_ServerMessageSummary 592
Report_SRPConnectivity 595
Report_UserMessageSummary 597
ResponseTime 600
ServerActivity 602
ServiceHealth 606
SRPConnectionStatus 613
SRPTest 616
UserActivity 618
UserCount 622
UsersWithPendingMessages 624

Chapter 15
BlackBerry Knowledge Scripts **627**
BesAlertForward 629
DebugLogTotalSize 632
EventLog 633
ExchangeAvail 634
HungThreads 635
MessagingServerList 636
MsgAvgSize 637
MsgBytesReceived 638
MsgsExpired 639
PurgeDebugLog 640
Report_EndToEndConnectivity 641

Report_EndToEndResponseTime 643
Report_ExchangeConnectionTime 645
Report_ExchangeConnectivity 647
Report_MessagesByInterval 649
Report_MessageSummary 651
Report_ServerList 654
Report_SRPConnectionUptime 656
Report_SRPConnectivity 658
Report_UserByServer 660
Report_UserListing 662
ResponseTime 664
ServerHealth 665
ServerLoad 666
ServicesDown 668
SNMPAlertForward 670
SRPConnectionStatus 672
SRPTest 673
UserCountByServer 674
UserList 675

Chapter 16
CallData Knowledge Scripts **677**
AddDataSource_CiscoCallMgr 679
AddDataSource_CiscoCM 682
AddDataSource_H323RADIUS 685
CancelDataCollection 689
CCME_GetConfig 690
ChangeReportingState 692
ChangeSchedule 693
ConfigureCallTypes 695
DataCollectionStatus 702
ExecuteDataCollection 703
RemoveDataSource 704
Report_CallAuthorization 705
Report_CallCompletionRate 708
Report_CallDetail_CiscoCallMgr 711
Report_CallDetail_H323Gateway 718
Report_CallFailureCauses 724
Report_CallJitter 733
Report_CallJitterLoss 736
Report_CallMOS 738
Report_CallPacketLoss 741
Report_CallQualityByPhone 744
Report_CallSuccessRate 747
Report_CallTraffic 750
Report_CallVolume 753
Report_CCME_StatsByEPhone 756
Report_CCME_Summary 759
Report_FrequentlyCalledNumbers 762
Report_GatewayDialPeers 765
Report_TrunkGroupByHour 768

Report_UnusedPhones....770
UpdateSecurity....772

Chapter 17
CallSetup Knowledge Scripts 775
H.323_CallSetup_Direct....776
H.323_CallSetup_Gatekeeper....777
H.323_CallSetup_Gateway....779
H.323_Listen....781
H.323_Registration....782
H.323_UpdateAlias....783
Report_H.323Configuration....784
Report_H.323ResponseAvailMatrix....785
Report_H.323ResponseTimeDetail....787
Report_SIPConfiguration....789
Report_SIPResponseAvailMatrix....790
Report_SIPResponseTimeDetail....792
SIP_CallSetup_Direct....794
SIP_CallSetup_Server....795
SIP_Listen....797
SIP_Registration....798
SIP_UpdateAlias....799

Chapter 18
CiscoCallMgr Knowledge Scripts 801
AnalogOutboundBusy....807
AnalogPortsActive....808
AnalogPortsOutOfService....809
CallActivity....810
CallFailures....811
CallQuality....820
CallsActive....825
CallsAttemptedByPhone....826
CallsInProgress....827
CCM_CheckFirmware....828
CCM_CpuHigh....830
CCM_DeviceStatus....831
CCM_EventLog....837
CCM_FXOPorts....839
CCM_FXSPorts....840
CCM_HealthCheck....841
CCM_HeartBeat....843
CCM_MemByProcess....844
CCM_MemoryHigh....846
CCM_MOHUnavailable....847
CCM_PhoneCheck....848
CCM_PhoneInventory....849
CCM_PRIChannels....855
CCM_Replication....856
CCM_ResetDevice....860

CCM_RestartService 863
CCM_RoleStatus 865
CCM_SecureWebPageCheck 866
CCM_SystemPerformance 868
CCM_SystemUsage 870
CCM_T1Channels 871
CCM_WebPageCheck 872
CDRQuery 874
CiscoBackupStatus 877
ConfBridgeActiveConf 878
ConfBridgeActiveStreams 879
ConfBridgeAvailStreams 880
ConfBridgeConferences 881
ConfBridgeStreams 882
CTI_Manager 883
DigitalOutboundBusy 884
DigitalPortsActive 885
DigitalPortsOutOfService 886
H323CallActivity 887
H323CallsAttempted 890
H323CallsInProgress 891
IIS_CpuHigh 892
IIS_HealthCheck 893
IIS_KillTopCPUProcs 894
IIS_MemoryHigh 895
IIS_RestartServer 896
IIS_ServiceUpTime 897
LineStatus 898
LocationBandwidth 899
LocationOutOfBandwidth 901
LossOfHardwarePhones 902
MGCP_FXO 904
MGCP_FXS 907
MGCP_Gateway_CCM30 910
MGCP_Gateway_CCM31 911
MGCP_GatewayCheck 913
MGCP_PRI 914
MGCP_PRI_Channels 917
MGCP_T1CAS 919
MGCP_T1CAS_Channels 922
MLA_Logins 924
MOHDevice 925
MOHServer 926
MOHServer_LostConnections 927
MTP_Device 928
MTPActiveConnections 929
MTPActiveStreams 930
MTPAvailableStreams 931
MTPCompletedConnections 932
MTPCompletedStreams 933
MTPsActive 934

MTPsAvailable 935
MTPsUnavailable 936
MulticastConfActive 937
MulticastConfAvailable 938
MulticastConfCompleted 939
MulticastConfPhones 940
MulticastConfUnavailable 941
QRTEvent 942
RegAnalogAccesses 943
RegCtiPorts 944
RegDigitalAccesses 945
RegHardwarePhones 946
RegMGCPGateways 947
RegOtherDevices 948
Report_CallActivity 949
Report_CallQualityDailyAvg 951
Report_CallsByHour 953
Report_ClusterAvgValueByHr 955
Report_ClusterAvgValueByMin 957
Report_ClusterGenCounter 959
Report_ClusterSystemUsage 961
Report_MGCPChannelUsage 963
Report_MGCPDeviceUtil 965
Report_MGCPGatewayUsage 967
Report_ServicesAvailability 969
Report_SystemUsage 971
SQL_Accessibility 973
SQL_BlockedProcesses 975
SQL_CPUUtil 976
SQL_DataGrowthRate 977
SQL_DataSpace 979
SQL_DBGrowthRate 981
SQL_DbOption 983
SQL_DBSpace 986
SQL_Errorlog 988
SQL_LogGrowthRate 989
SQL_LogSpace 991
SQL_MemUtil 993
SQL_NearFileMaxSize 994
SQL_NearMaxConnect 996
SQL_NearMaxLocks 997
SQL_NetError 998
SQL_RepTransactions 999
SQL_RepTranSec 1000
SQL_RestartServer 1001
SQL_ServerDown 1002
SQL_ServerThroughput 1003
SQL_TopIOUsers 1004
SQL_TopLockUsers 1005
SQL_TopMemoryUsers 1006
SQL_UserConnections 1007

StreamAppIOCTLErr....1008
StreamAppMissDDErr....1009
TftpChangeNotify....1010
TftpErrors....1011
TftpHeartBeat....1012
TftpRequests....1013
TftpSegmentPctLost....1014
TftpSegmentsSent....1015
TraceArchive....1016
TraceEvent....1017
Transcoder_Device....1018
TranscoderResources....1019
TranscoderUnavailable....1020
UnicastConfActive....1021
UnicastConfAvailable....1022
UnicastConfBridge_Device....1023
UnicastConfComplete....1025
UnicastConfParticipants....1026
UnicastConfUnavailable....1027
VerifyPasswords....1028
Recommended Knowledge Script Groups....1030

Chapter 19
CiscoCM Knowledge Scripts 1033
4x_PhoneDeregistrations....1036
4x_RetrieveConfigData....1038
4x_SetupSupplementalDB....1039
AnalogAccess_GatewayUsage....1040
Annunciator_Device....1042
AttendantConsole....1044
CCM_CallActivity....1046
CCM_MediaResources....1049
CCM_MGCPResources....1054
CCM_RegisteredResources....1057
CCM_ResourceAvailability....1062
CCM_SystemPerformance....1067
CDR_CallFailures....1071
CDR_CallQuality....1080
CDR_Query....1084
CDR_RetrieveCallRecords....1086
CDR_RetrieveConfigData....1087
CFB_Hardware_Device....1088
CFB_Software_Device....1090
CFB_Video_Device....1092
CTIManager....1094
ExtensionMobility....1096
GatekeeperActivity....1098
GeneralCounter....1100
H323_Gateway_CallActivity....1102
H323_Trunk_CallActivity....1104
HealthCheck....1106

HuntAndRouteList....1108
Locations....1110
MediaStreamingApp....1112
MGCP_FXO_CallActivity....1116
MGCP_FXS_CallActivity....1118
MGCP_GatewayUsage....1120
MGCP_PRI_CallActivity....1123
MGCP_PRI_ChannelHealth....1125
MGCP_T1CAS_CallActivity....1126
MGCP_T1CAS_ChannelHealth....1128
MOH_Device....1129
MTP_Device....1131
PhoneDeregistrations....1133
PhoneInventory....1135
Report_PhoneDeregAudit....1138
Report_PhoneDeregWatchList....1141
RoleStatus....1143
SetupSupplementalDB....1144
SIP_Trunk_CallActivity....1147
SNMPTrap_AddMIB....1149
SNMPTrap_Async....1151
SystemUpTime....1158
SystemUsage....1159
TFTPActivity....1163
Transcoder_Device....1166
WebDialer....1168
WebPageCheck....1170
Recommended Knowledge Script Group....1172
Troubleshooting Missing Data Points....1173

Chapter 20
CiscoCME Knowledge Scripts 1175
Device_Reset....1176
Device_Status....1178
Extension_Check....1181
Phone_Inventory....1182
Set_Key_Phones....1184
SRST_Failover....1186

Chapter 21
CiscoICD Knowledge Scripts 1187
AgentsLoggedOn....1189
CallStatistics....1190
CSQ_ServiceLevel....1193
ICD_CpuHigh....1195
ICD_EventLog....1198
ICD_HealthCheck....1200
ICD_MemoryHigh....1202
ICD_RestartService....1207
ICD_SystemUsage....1210

IIS_CpuHigh 1212
IIS_HealthCheck 1213
IIS_KillTopCPUProcs 1214
IIS_MemoryHigh 1215
IIS_ServiceUpTime 1216
SQL_Accessibility 1217
SQL_CPUUtil 1219
SQL_DataGrowthRate 1220
SQL_DBGrowthRate 1222
SQL_MemUtil 1224
SQL_RestartServer 1226
Recommended Knowledge Script Group 1227

Chapter 22
CiscoICM Knowledge Scripts 1229
ICM_AgentData 1231
ICM_Alarms 1233
ICM_EventGetViaFilter 1235
ICM_EventLog 1236
ICM_ProcessLog 1238
ICM_RouteData 1240
ICM_RoutingClientData 1243
ICM_ScheduledTargetDataLocal 1246
ICM_ScriptData 1248
ICM_ServiceData 1250
ICM_ServiceDataLocal 1253
ICM_SkillGroupData 1256
ICM_SkillGroupDataLocal 1259
IIS_CpuHigh 1261
IIS_HealthCheck 1262
IIS_KillTopCPUProcs 1263
IIS_MemoryHigh 1264
IIS_RestartServer 1265
IIS_ServiceUpTime 1266
Router_AgentsLoggedOn 1267
Router_CallsInProgress 1268
Router_CallsPerSec 1269
SQL_Accessibility 1270
SQL_CPUUtil 1272
SQL_DataGrowthRate 1273
SQL_DBGrowthRate 1274
SQL_MemUtil 1276
SQL_RestartServer 1277
Recommended Knowledge Script Group 1278

Chapter 23
CiscoIPT Security Knowledge Scripts 1279
CCM_MaliciousCalls 1280
CCM_MemoryConsumption 1281
CCM_ServiceFailure 1284

CCM_TransientConnects 1285
CCM_UnauthorizedCalls 1286
CPUHigh 1287
CSA_Events 1288
CSA_HealthCheck 1290
Ettercap_Detect 1292
LoginFailures 1293
MemoryHigh 1295
ServiceFailure 1296
Symantec_Events 1297
Symantec_HealthCheck 1299
VerifyHotfix 1301

Chapter 24
CiscoIVR Knowledge Scripts **1303**
IIS_CpuHigh 1304
IIS_HealthCheck 1305
IIS_KillTopCPUProcs 1306
IIS_MemoryHigh 1307
IIS_RestartServer 1308
IIS_ServiceUpTime 1309
IVR_CpuHigh 1310
IVR_EventLog 1311
IVR_HealthCheck 1314
IVR_MemoryHigh 1315
IVR_RestartService 1316
IVR_SystemUsage 1317
Report_ServicesAvailability 1318
Report_SystemUsage 1320

Chapter 25
CiscoUnity Knowledge Scripts **1323**
CU_BackupAndRestoreStatus 1325
CU_CallActivity 1326
CU_CpuHigh 1328
CU_CurrentDiskQueueLength 1330
CU_EventLog 1331
CU_FailoverStatus 1333
CU_HealthCheck 1335
CU_LicenseCompliance 1337
CU_MemoryHigh 1338
CU_MessageDeliveryFailure 1342
CU_MessageStoreAvailability 1343
CU_MessageStoreLock 1344
CU_NumberOfLogons 1345
CU_PortStatus 1346
CU_ProcessorQueueLength 1347
CU_RestartService 1348
CU_Silence 1350
CU_SystemUsage 1351

CU_TTSPortsInUse 1352
CU_UMRServiceHung 1353
CU_VoicePortsInUse 1354
IIS_CpuHigh 1355
IIS_HealthCheck 1356
IIS_KillTopCPUProcs 1357
IIS_MemoryHigh 1358
IIS_RestartServer 1359
IIS_ServiceUpTime 1360
Report_PortUsage 1361
Report_ServicesAvailability 1363
Report_SystemUsage 1365
SQL_Accessibility 1367
SQL_CPUUtil 1369
SQL_DataGrowthRate 1370
SQL_DBGrowthRate 1371
SQL_MemUtil 1373
SQL_RestartServer 1374
Recommended Knowledge Script Groups 1375
Discovery_CiscoUnity 1376

Chapter 26
CiscoUnityBridge Knowledge Scripts 1377
CUB_CpuHigh 1378
CUB_EventLog 1379
CUB_HealthCheck 1381
CUB_MemoryHigh 1382
CUB_RestartService 1383
CUB_SystemUsage 1384
IIS_CpuHigh 1385
IIS_HealthCheck 1386
IIS_KillTopCPUProcs 1387
IIS_MemoryHigh 1388
IIS_RestartServer 1389
IIS_ServiceUpTime 1390
Report_ServicesAvail 1391
Report_SystemUsage 1393

Chapter 27
CiscoUE Knowledge Scripts 1395
BackupAndRestoreStatus 1396
DeviceUptime 1397
GDMStorageUsage 1398
LicenseCompliance 1399
MessageActivity 1401
OrphanedMailboxes 1403
PortStatus 1404
SubscriberStorageUsage 1405
SystemUsage 1406
TotalStorageUsage 1407

VoiceMailLogins 1408
VoiceMailSessionsInUse 1411
Recommended Knowledge Script Group 1413

Chapter 28
CiscoPA Knowledge Scripts **1415**
CPA_CallActivity 1417
CPA_CallsTransferredToDTMF 1418
CPA_CpuHigh 1419
CPA_DialByName 1421
CPA_EventLog 1422
CPA_FalseAcceptance 1424
CPA_HealthCheck 1425
CPA_LogInFailure 1427
CPA_MemoryHigh 1428
CPA_NonSpeechSessions 1430
CPA_RestartService 1431
CPA_Sessions 1433
CPA_SpeechChannelCreateFailure 1434
CPA_SpeechRecognitionFailure 1435
CPA_SystemUsage 1436
CPA_TransferFailed 1437
CPA_VoiceMail 1438
IIS_CpuHigh 1439
IIS_HealthCheck 1440
IIS_KillTopCPUProcs 1441
IIS_MemoryHigh 1442
IIS_RestartServer 1443
IIS_ServiceUpTime 1444
Report_CallActivity 1445
Report_ServicesAvailability 1447
Report_SystemUsage 1449

Chapter 29
Citrix MetaFrame Knowledge Scripts **1451**
ApplicationUsersHigh 1453
BytesTransferredPerUser 1454
DataCollectorChanged 1455
DefaultDataCollector 1456
FarmUserLoad 1457
ICAAvgLatencyHigh 1459
ICALatencyHigh 1460
LicenseInUseHigh 1461
PublishedApplicationDetails 1463
ServerFarmHealth 1464
ServerProcessesHigh 1467
ServerProcessesResourceHigh 1468
ServerSessionsHigh 1470
SessionPerUser 1471
SessionState 1472

UserResourcesHigh 1474

Chapter 30
Dell OpenManage Knowledge Scripts **1477**
AdapterSCSI 1478
AmperageProbe 1479
ArrayLogicalDrive 1480
ArrayPhysicalDrive 1481
EventLog 1482
FanProbe 1483
HealthCheck 1484
MemCheck 1485
NICError 1486
NICFail 1487
PowerRedundancy 1488
PowerSupply 1489
Report_AmperageProbe 1490
Report_ArrayLogicalDrives 1493
Report_ArrayPhysicalDrives 1496
Report_FanProbe 1499
Report_NICErrorRate 1502
Report_TemperatureProbe 1505
Report_VoltageProbe 1508
TempProbe 1511
VoltageProbe 1512

Chapter 31
Diag Knowledge Scripts **1513**
RetrieveData 1514
StartCollectionAD 1515
StartCollectionExchange 1516
StartCollectionNT 1517

Chapter 32
Discovery Knowledge Scripts **1519**
Discovering Application Resources 1524
Discovering Clustered Applications 1525
ActiveDS 1528
AD-RT 1533
AMHealth 1534
AMHealthUNIX 1536
ApacheUNIX 1537
AppAnalyzer 1538
Application 1539
ARCserve 1541
AvayaCM 1542
BackupExec 1547
BES 1548
BlackBerry 1550
BlackBerry-Domino 1551

Brocade (BRCD) 1552
CallDataAnalysis 1553
CIM 1554
CiscoCallMgr 1556
CiscoCM 1558
CiscoCM_4x 1562
CiscoCME 1564
CiscoCNS_PerfE 1568
CiscoICD 1570
CiscoICM 1571
CiscoICS 1572
CiscoIPTSecurity 1573
CiscoIPTV 1574
CiscoIVR 1575
CiscoPersonalAsst 1576
CiscoUE 1577
CiscoUnity 1581
CiscoUnityBridge 1582
Cluster 1583
Dell 1585
Domino 1586
Domino-RT 1588
Exchange 1589
Exchange2007 1590
ExchangeDAG 1591
Exchange-RT 1592
HIS 1593
HPNS 1594
IIS 1595
ISA 1596
MFXP 1597
ModuleBuilder 1598
MOMReportAgent 1599
MQSeries 1600
MSCS 1601
MSMQ 1602
MTS 1603
NetAppFiler 1604
NetBackup 1605
NetBackupUNIX 1606
Netfinity 1607
NetfinityDir 1608
NetworkDevice 1609
NetWorker 1614
Networks-RT 1615
Networks-RTProxy 1616
NortelBCM 1618
NortelBCMx 1619
NortelBCM50x 1621
NortelCC 1623
NortelCS 1625

NortelCS2x 1629
NT 1637
OCS 1638
Oracle 1639
Oracle-RT 1641
OracleUNIX 1642
PhoneQuality 1643
Proxy 1644
ReportAgent 1645
SAP 1647
SAPITS 1649
ScanMailExch 1650
Security 1651
SharePoint 1653
SharePoint2010 1654
Siebel 1655
Siemens 1657
SNA 1658
Snmp 1659
SQL 1663
SQL-RT 1664
StreamingMedia-RT 1665
UNIX 1666
VirtualCenter 1667
VoIPQuality_CallPerf 1670
VoIPQuality_CallPerfProxy 1671
VoIPQuality_CallSetup_H.323 1672
VoIPQuality_CallSetup_SIP 1673
VoIPQuality_CiscoSAA 1674
Web-RT 1676
WebLogicSvr 1677
WebLogicSvrUNIX 1679
WebServices 1681
WebSphereAppSrv 1682
WebSphereAppSrvUNIX 1685
WebSphereMQUNIX 1688
Win-RT 1689
Win-RT7 1691
WLBS 1693
WMI 1694
WRC 1695
WS.NET 1696
WTS 1698
XenApp 1699
Antigen 1700
AppCenter 1701
BizTalk 1702
Commerce 1703
Conference 1704
FW1 1705
NetShield 1706

NetwareManager 1707
Site 1708
SMS 1709

Chapter 33
Domino Knowledge Scripts **1711**
Connectivity 1713
ConsoleCommand 1716
CPUUtil 1718
DbACLChanged 1720
DBCacheHit 1722
DBDocNumber 1724
DBReplicating 1726
DBSizes 1728
DBWhiteSpace 1730
GetStat 1732
HTTPAccessStat 1734
InetPortCheck 1736
LogSniff 1738
MailThruput 1740
MemBusy 1743
NetworkBusy 1745
NotesMailStats 1747
OldestDocInDB 1750
OpenDBResponseTime 1752
ReplicationTime 1754
Report_Connectivity 1756
Report_DatabaseSize 1758
Report_MailThroughputDeadMails 1761
Report_MailThroughputFailureMail 1764
Report_MailThroughputPendingMails 1767
Report_MailThroughputRoutedMail 1770
Report_MailThruputDeliveredMail 1773
Report_ServerDown 1776
Report_ServerUpTime 1778
Report_TopNDatabases 1780
Report_UserSessions 1781
ServerAvailability 1784
ServerDown 1786
SMTPConnectivity 1788
TaskAvailability 1791
TaskDown 1794
TopNAccessDbs 1796
TopNDatabases 1798
TopNMailDatabases 1800
TopNUnUsedDBs 1802
TopNUsers 1804
UserSessions 1806

Chapter 34
Exchange and Exchange2000 Knowledge Scripts 1809
CategorizerHealth 1813
CategorizerMessages 1815
ClusterOwner 1817
Connectivity 1818
ConnectorStatus 1823
DynSecsOldestMsgInMTAQueue 1824
IMAP4Accesses 1825
IMAP4Authenticate 1826
IMAP4Connections 1827
InactiveMailboxes 1828
InactivePublicFolders 1830
ISConnections 1832
ISLogFileSize 1833
ISMailboxStoreAvgDlvryTime 1834
ISMailboxStoreOpens 1835
ISMailboxStoreSize 1836
ISPubStoreAvgDeliveryTime 1837
ISPubStoreOpens 1838
ISPubStoreSize 1839
LinkStatus 1840
LogParser 1842
MailboxesOverStorageLimit 1850
MailboxesWithoutStorageLimit 1852
MailboxStoreMountStatus 1854
MsgAvgLocalDlvryTimeByIntrv 1855
MsgsAvgLocalDeliveryTime 1856
MsgsBetweenAdminGroups 1857
MsgsBtwnAdmnGrpsByInterval 1859
MsgsByServer 1861
MsgsByServerByInterval 1863
MsgsBySize 1865
MsgsOfSystem 1867
MsgsOpenedByOWA 1869
MsgsSentByOWA 1870
MsgsSpecificDomain 1871
MsgsSpecificDomainByInterval 1873
MsgsThroughConnector 1874
MsgsThroughSMTPService 1876
MsgsThruSMTPSvcByInterval 1877
MsgsWithinAdminGroup 1878
MsgsWthnAdmnGrpByInterval 1880
MTAConnectionQueueLength 1881
NNTPConnections 1883
NumberOfMailboxes 1884
PFAclChanges 1886
PFAclInfo 1887
PFInfo 1888
PFReplicationByObj 1891
POP3Accesses 1893

POP3Authenticate 1894
POP3Connections 1895
ProtocolVSStatus 1896
PublicStoreMountStatus 1897
QueueStatus 1898
Report_Connectivity 1900
Report_ISPrivateResourceSummary 1902
Report_ISPublicResourceSummary 1905
Report_ServerLoad 1908
Report_ServerMessage 1910
Report_ServerUsers 1912
Report_TopNMailboxesInfo 1914
Report_TopNReceivers 1916
Report_TopNSenders 1918
ResponseTime 1920
ServerHealth 1923
ServerHistory 1925
ServerLoad 1927
ServerQueues 1929
ServerTotalMsg 1930
ServerUsers 1932
ServicesDown 1933
SMTPConnectivity 1935
SMTPConnectivityEx 1941
SRSServiceDown 1945
TopNISMailboxRes 1946
TopNISPublicRes 1948
TopNReceivers 1950
TopNSenders 1952

Chapter 35
Exchange 2007 Knowledge Scripts **1955**
All_BestPracticesAnalyzer 1957
All_ClockSynchronization 1960
All_EventLog 1961
All_ServiceStatus 1962
CAS_Activity 1964
CAS_Connectivity 1970
CAS_OABAvailability 1974
CAS_PublicFolderAvailability 1975
ETS_ExternalMail 1976
ETS_MessageHygiene 1979
HTS_Connectivity 1982
HTS_SendersAndRecipients 1984
HTS_TransportDumpster 1987
MBS_ClusterOwner 1989
MBS_DatabaseStateChange 1990
MBS_DatabaseStatus 1993
MBS_MailboxAccessibility 1996
MBS_MailboxUsage 1998
MBS_MailFlow 2000

MBS_MessagingRecordsMgmt 2001
MBS_PublicFolderUsage 2004
MBS_Replication 2006
Transport_BackPressure 2009
Transport_QueueStatus 2011
UMS_CallActivity 2015
UMS_Connectivity 2018
UMS_Failures 2020
UMS_Performance 2023
Recommended Knowledge Script Group 2026

Chapter 36
Exchange-RT Knowledge Scripts **2029**
CheckAddressBookEntry 2030
OpenFolder 2035
OpenFolderAndRead 2040
SendAndReceiveMessage 2045
SendAndTrackMessage 2050
Report_Exchange-RT 2055

Chapter 37
General Knowledge Scripts **2057**
Creating Filters with Regular Expressions 2059
ADAuthentication 2061
AsciiLog 2063
AsciiLogRX 2066
ConfigMachineDown 2068
Counter 2069
CounterCorrelate 2073
EventLog 2075
EventLogRX 2079
MachineDown 2084
MachineDownLR 2090
MissingEvent 2092
PingMachine 2097
Report_MachineAvailability 2099
Report_PingMachine 2101
Report_ServiceChange 2103
Report_ServiceDown 2105
Report_ServiceHung 2107
ServiceChange 2109
ServiceDown 2110
ServiceHung 2112
ShortEventLog 2113
SNMPGet 2117
WMICounter 2119

Chapter 38
HP SIM Knowledge Scripts **2123**
ArrayLogicalDriveCondition 2125

ArrayLogicalDriveStatus 2126
ArrayPhysicalDiskStatus 2128
ASRHealth 2129
ASRStatus 2130
CorrectableMem 2131
CriticalErrorLog 2132
EventLog 2133
FanIndividual 2135
FanSummary 2136
FCAExternalControllerFail 2137
FCAFail 2138
FCAHostControllerFail 2139
FCAHostFail 2140
FCAOverallCondition 2141
FLTPWRIndividualCondition 2142
FLTPWROverallCondition 2143
HealthCheck 2144
IDAFail 2145
IDEFail 2146
IntegratedLog 2147
NICError 2148
NICFail 2149
Report_ASRHealth-RebootCount 2150
Report_CIMResource_CPU_MemoryUsage 2152
Report_CIMSCSI-Status 2155
Report_CorrectableMemoryErrors 2158
Report_NewEventLogEntries 2160
Report_NICErrorRate 2162
ResourceHigh 2165
RIBBatteryRechargeLevel 2166
RIBBatteryStatus 2167
RIBCableConnections 2168
RIBCondition 2169
RIBInterfaceStatus 2170
RIBVirtualPowerCable 2171
SCSIFail 2172
SCSITimeout 2173
TeamedNICCondition 2174
TempIndividual 2175
ThermalStatus 2176
UPSBatteryLow 2177
UPSLineStatus 2178

Chapter 39
IBM Systems Director Knowledge Scripts 2179

EventLog 2180
FanSpeed 2182
HealthCheckHW 2184
HealthCheckMgmtSrv 2185
MemoryErrors 2186
NICError 2187

ServeRAIDControllerStat....2188
ServeRAIDLogicalDriveStat....2189
ServeRAIDPhysicalDrivePFA....2190
ServeRAIDPhysicalDriveStat....2191
Temperature....2192
Voltage....2194
Discovery_NetfinityDir....2195

Chapter 40
IIS Knowledge Scripts 2197
ApplicationPools....2203
ASPCommFailure....2204
ASPEventLog....2205
ASPNETApplicationRestarted....2208
ASPNETApplicationRunning....2209
ASPNETErrors....2210
ASPNETPipelineInstances....2211
ASPNETReqStat....2212
ASPNETRequestCurrent....2215
ASPNETRequestDisconnected....2216
ASPNETRequestExecuteTime....2217
ASPNETRequestQueued....2218
ASPNETRequestRate....2219
ASPNETRequestRejected....2220
ASPNETRequestWaitTime....2221
ASPNETWorkerProcessCPU....2222
ASPNETWorkerProcessExcepRate....2223
ASPNETWorkerProcessExceptions....2224
ASPNETWorkerProcessMemory....2225
ASPNETWorkerProcessRestarted....2226
ASPNETWorkerProcessRunning....2227
ASPQueueBusy....2228
ASPRegistryChange....2229
ASPReqStat....2230
ASPRequestError....2232
ASPRequestFailed....2233
ASPSessionTimeout....2234
ASPThroughput....2235
CacheHitRatio....2236
CentralizedBinaryLogging....2237
CGIRequests....2239
CpuHigh....2240
FTPBytes....2241
FTPConnections....2242
FTPConnectionsInterval....2243
FTPConnectionUtil....2244
FTPFiles....2245
FTPStatistics....2246
FTPTransStat....2248
HealthCheck....2250
HTTPBytes....2251

HTTPBytesInterval 2252
HTTPConnectionsInterval 2254
HTTPConnectionUtil 2256
HTTPFiles 2257
HTTPNotFound 2259
HTTPRequests 2260
HTTPStatistics 2262
HTTPTransStat 2264
IsolatedApps 2266
KillTopCPUProcs 2268
Log 2269
MemoryHigh 2271
NNTPArticles 2273
NNTPBytes 2274
NNTPClientCommands 2275
NNTPClientFailures 2277
NNTPConnections 2278
NNTPConnectionsInterval 2279
NNTPConnectionUtil 2280
NNTPEventLog 2281
NNTPServerFailures 2284
NNTPSpaceLow 2285
NNTPStatistics 2286
Report_ASPCommunicationFailure 2288
Report_ASPNETApplicationRestarted 2291
Report_ASPNETApplicationRunning 2294
Report_ASPNETErrors 2297
Report_ASPNETPipelineInstances 2300
Report_ASPNETReqStat 2303
Report_ASPNETRequestCurrent 2306
Report_ASPNETRequestDisconnected 2309
Report_ASPNETRequestExecuteTime 2312
Report_ASPNETRequestQueued 2315
Report_ASPNETRequestRate 2318
Report_ASPNETRequestRejected 2321
Report_ASPNETRequestWaitTime 2324
Report_ASPNETWorkerProcessCPU 2327
Report_ASPNETWorkerProcessExcepRate 2330
Report_ASPNETWorkerProcessExceptions 2333
Report_ASPNETWorkerProcessMemory 2336
Report_ASPNETWorkerProcessRestarted 2339
Report_ASPNETWorkerProcessRunning 2342
Report_ASPNewEventLogEntries 2345
Report_ASPQueueBusy 2348
Report_ASPRegistryChange 2351
Report_ASPReqStat 2354
Report_ASPRequestError 2357
Report_ASPRequestFailed 2360
Report_ASPSessionTimeout 2363
Report_ASPThroughput 2366
Report_CpuUsage 2369

Report_FTPBytesRate....2372
Report_FTPConnections....2375
Report_FTPFilesTransferRate....2378
Report_FTPTransStat....2381
Report_HTTPC21WebTransferRate....2384
Report_HTTPNotFoundError....2387
Report_MemoryUsage....2390
Report_NNTPArticlesTransferRate....2393
Report_NNTPBytesTransferRate....2396
Report_NNTPClientCommands....2399
Report_NNTPClientFailures....2402
Report_NNTPCurrentConnections....2405
Report_NNTPTransStat....2408
Report_NNTPVirtualRootDiskSpace....2411
RestartServer....2414
ServiceUptime....2415
SMTPBytesInterval....2416
SMTPConnections....2417
SMTPConnectionsInterval....2418
SMTPConnectionUtil....2419
SMTPMsgs....2420
SMTPQueue....2422
SMTPStatistics....2423
SSLCertMon....2425
UDDIConnections....2426
UnloadApps....2427
WebServiceExtensions....2428

Chapter 41
Module Builder Knowledge Scripts 2429
Generating Knowledge Scripts for a New Module....2430
Working with Module Builder Knowledge Scripts....2431
Revising an Existing Module Builder Custom Module....2432
Using the Browse Button to Set Parameters....2433
EventLogCheck....2434
LogFileCheck....2437
PerformanceMetrics....2440
ProcessHealthCheck....2442
ServiceHealthCheck....2447
Discovery_ModuleBuilder....2453

Chapter 42
MSCS Knowledge Scripts 2455
EventLog....2456
GroupDown....2458
GroupOwnerChange....2459
HealthCheck....2460
NetInterfaceDown....2462
NetworkDown....2463
NodeDown....2464

ResourceDown....2465
ResourceOwnerChange....2466

Chapter 43
NetBackupUNIX Knowledge Scripts 2467
Clients....2468
DBDirSize....2469
DeviceStatus....2470
ErrorLog....2471
FailedJobs....2472
IncompleteJobs....2473
LogDirSize....2474
PendingRequest....2475
ResourceHigh....2476
StorageUnitsChanged....2477
SuccessfulJobs....2478

Chapter 44
NetBackup Knowledge Scripts 2479
Clients....2480
DBDirSize....2481
DeviceStatus....2482
ErrorLog....2483
EventLog....2484
FailedJobs....2486
IncompleteJobs....2487
LogDirSize....2488
PendingRequest....2489
ResourceHigh....2490
ServiceDown....2491
StorageUnitsChanged....2492
SuccessfulJobs....2493

Chapter 45
NetServices Knowledge Scripts 2495
DHCPHealthCheck....2496
DHCPLeases....2497
DNSHealthCheck....2499
DNSSync....2501
RASConnections....2502
RASErrors....2503
RASHealthCheck....2504
RASStat....2505
WINSConflict....2506
WINSFailure....2507
WINSHealthCheck....2508
WINSQueries....2509
WINSReplication....2510
WINSStat....2511

Chapter 46
NetworkDevice Knowledge Scripts 2513
ATMLink_QoS....2515
ATMLink_Util....2518
Chassis_Usage....2520
Device_Ping....2524
Device_Syslog....2525
Device_Uptime....2527
FrameRelayLink_QoS....2528
FrameRelayLink_Util....2531
FXOPort_Health....2533
FXOPort_Util....2534
FXSPort_Health....2535
FXSPort_Util....2536
Host_CPULoaded....2537
Host_DeviceStatus....2538
Host_MemoryUsage....2539
Host_ProcessDown....2540
Host_ProcessUp....2541
Host_StorageUsage....2542
Interface_Health....2543
IPSubsystem_Util....2546
ISDNChannel_CallVolume....2547
ISDNChannel_Health....2548
ISDNChannel_Util....2550
LANLink_QoS....2551
LANLink_Util....2554
Report_ChassisUsage....2556
Report_DeviceAvailability....2558
Report_ISDNCallVolume....2560
Report_ISDNTimeDetail....2562
Report_ISDNUtilization....2564
Report_LinkUtilization....2566
Report_QoSUtilization....2568
Report_QoSVolume....2570
Report_TotalVolume....2572
SingleATMLink_Util....2574
SingleFrameRelayLink_Util....2576
SingleInterface_Health....2578
SingleLANLink_Util....2579
SingleWANLink_Util....2581
SNMPTrap_AddMIB....2583
SNMPTrap_Async....2585
WANLink_QoS....2590
WANLink_Util....2593
Recommended Knowledge Scripts....2595

Chapter 47
Networks-RT Knowledge Scripts 2597
[ResponseTime]....2602

[Throughput] 2604
Action_Traceroute 2606
Action_TracerouteNetworks-RT 2608
ActiveDirectoryAddUser 2610
ActiveDirectoryLogin 2612
ActiveDirectoryReplication 2614
ActiveDirectoryResetPassword 2616
BaanAddItem 2618
BaanGenerateMPSMRPBatches 2620
BaanLoadDEM 2622
BaanLoadItemMaster 2624
BaanMaintainCustomer 2626
BaanMaintainEmployeeAdd 2628
BaanMaintainProductBom 2630
BaanMaintainPurchaseOrder 2632
BaanMaintainSalesOrder 2634
BaanMaintainServiceOrder 2636
BaanPrintCompaniesListSelect 2638
BackWebSignupAndInfoPakDnld 2640
BackWebUpdate 2642
CastanetChannelDownload 2644
CastanetInitialRun 2646
ccMail 2648
CitrixICAExcelStartup 2650
CitrixICAIEStartup 2652
CitrixICAOutlookOpenFullBox 2654
CitrixICATerminalServerLogon 2656
CitrixICAWordStartUp 2658
CreditCheckShortConnection 2660
DatabaseUpdateShortConnect 2662
DNSNameLookup 2664
ExchangeDirectoryService 2666
ExchangeReadMail 2668
ExchangeReceiveMail 2670
ExchangeSendMail 2672
FileReceiveShortConnection 2674
FileSendShortConnection 2676
FTPGet 2678
FTPPut 2680
HeadlinerInitialLoad 2682
HeadlinerSubsequentUpdate 2684
HTTPGIFTransfer 2686
HTTPSSecureTransaction 2688
HTTPTextTransfer 2690
InquiryShortConnection 2692
LDAPDirectoryLookup 2694
MicrosoftRDPExcelStartUp 2696
MicrosoftRDPIEStartLoadMSN 2698
MicrosoftRDPOutlookOpenBox 2700
MicrosoftRDPTermServerLogon 2702
MicrosoftRDPWordStartUp 2704

MSSQLQuery 2706
NetworkNewsTransferProtocol 2708
NotesAttachOpenDB 2710
NotesAttachOpenInitDB 2712
NotesAttachServerDetach 2714
NotesAttachServers2Detach 2716
NotesBrowserDBAttach 2718
NotesBrowserDBOpen 2720
NotesBrowserDBSearch 2722
NotesCheckForUnreadEmail 2724
NotesCreateSaveMailNote 2726
NotesCreateSaveSendAttach 2728
NotesCreateSaveSendMailNote 2730
NotesCreateTextIndexServer 2732
NotesIndexedDBLookup 2734
NotesNonIndexedDBLookup 2736
NotesReceiveEmail 2738
NotesReplicateMail 2740
NotesReplicateServer1DB 2742
NotesReplicateServer50Auto 2744
NotesReplicateServer50Docs 2746
NotesReplicateServerCheck 2748
NotesSendEmail 2750
NTFilePrintPrintaFile 2752
OracleAPTier1FindInvoice 2754
OracleAPTier1InvoiceMultDist 2756
OracleAPTier2FindInvoice 2758
OracleAPTier2InvoiceMultDist 2760
OracleARTier1InsertCustomer 2762
OracleARTier1ViewCustomer 2764
OracleARTier2InsertCustomer 2766
OracleARTier2ViewCustomer 2768
OracleFATier1AssetInquiry 2770
OracleFATier1ManualAddition 2772
OracleFATier2AssetInquiry 2774
OracleFATier2ManualAddition 2776
OracleGLTier1AccountInquiry 2778
OracleGLTier1JournalEntry 2780
OracleGLTier2AccountInquiry 2782
OracleGLTier2JournalEntry 2784
PacketBlasterLongConnection 2786
PacketBlasterRevLongConnect 2788
PointCastv1InitialUpdate 2790
PointCastv2InitialUpdate 2792
POP3ReceiveEmail 2794
SAPR3AuthPaymentOnInvoice 2796
SAPR3BasicStock 2798
SAPR3BatchCharacterizeStock 2800
SAPR3CreatePurchaseOrder 2802
SAPR3CreateSalesOrder 2804
SAPR3GoodsReceipt 2807

SAPR3GoodsReceiptInspection....2809
SAPR3Login....2811
SAPR3MaterialToMaterialXfer....2813
SAPR3PickingBatchDetermine....2815
SAPR3PostGoods....2818
SAPR3PrepareAnInvoice....2820
SAPR3QMResultsRecording....2822
SAPR3SalesOrderDelivery....2825
SMTPSendEmail....2828
Telnet....2830
Traceroute....2832
Report_ResponseTimeSummary....2834
Report_ThroughputSummary....2837
Report_TracerouteException....2840
Report_TracerouteProfile....2844
Net-RT-Import_KSGenerator....2848

Chapter 48
NortelBCM Knowledge Scripts 2857
BCM_HealthCheck....2859
BCM_QoSInterfaceActivity....2861
BCM_QoSLog....2862
BCM_QoSPrioritySessions....2863
BCM_QoSQueueUsage....2864
BCM_SystemUsage....2866
Report_ServicesAvailability....2867
Report_SystemUsage....2869
Sys_AsciiLog....2871
Sys_CpuByProcess....2873
Sys_CpuLoaded....2874
Sys_DNSConnectivity....2875
Sys_EventLog....2876
Sys_FailedLogon....2879
Sys_FileChanged....2881
Sys_FilesCompare....2882
Sys_GeneralCounter....2883
Sys_IntervalCounter....2887
Sys_LogicalDiskSpace....2889
Sys_MemUtil....2890
Sys_PagingHigh....2891
Sys_ProcessDown....2892
Sys_Processes....2893
Sys_ServiceChange....2894
Sys_ServiceDown....2895
Sys_ServiceHung....2896
Sys_SystemUpTime....2897
Sys_TopCpuProcs....2898
Sys_TopMemoryProcs....2899

Chapter 49
NortelBCMx Knowledge Scripts 2901
Alarms 2902
CallByCallLimits 2905
ChassisUsage 2908
HealthCheck 2916
HuntGroupUsage 2920
InterfaceHealth 2922
LinkUtilization 2923
LogicalDiskSpace 2926
PSTNFallback 2928
QoSLog 2930
SystemUpTime 2934
SystemUsage 2935
UPSHealth 2937
Recommended Knowledge Script Group 2940
Discovery_NortelBCMx 2941

Chapter 50
NortelCC Knowledge Scripts 2943
AgentTimes 2944
Alarms 2947
CallsAbandoned 2949
CallsAnswered 2953
CallsConfTrans 2958
CallsOffered 2961
CallsTerminated 2962
CallTimes 2964
CallTreatments 2969
Database 2976
HealthCheck 2978
SkillsetTimes 2980
SystemUsage 2982

Chapter 51
NortelCS Knowledge Scripts 2985
Alarms 2986
BMZ_CallQuality 2995
CallCapacity 3001
GetOMReport 3003
HealthCheck 3007
PhoneInventory 3009
SS_CallQuality 3011
SS_H323Stats 3017
SS_Registration 3019
SS_SIPStats 3021
VGMC_CallQuality 3023

Chapter 52
NortelCS2x Knowledge Scripts **3025**
AddPhone 3026
CallActivity 3028
CallAlert....3031
CallFailures 3034
CallQuality....3039
CollectorHealth 3044
LogQuery 3047
OMQuery....3050
PhoneDiagnostic....3053
PhoneInventory 3055
PhoneQuality....3057
RemovePhone....3061
RetrieveConfigData 3062
SetupSupplementalDB 3063
Recommended Knowledge Script Group 3066
Triggering Call and Phone Quality Diagnoses....3067

Chapter 53
NT Knowledge Scripts **3069**
ConfigRemoteServiceDown 3072
ConfigServiceDown....3073
CpuByProcess 3074
CpuLoaded 3076
CpuResource....3079
DiskSpace....3080
DNSConnectivity....3083
FailedLogon 3084
FileChanged....3085
FilesCompare....3087
FileSizeSum....3088
FilesOpen....3090
FindFiles....3091
FolderFileCount 3093
FolderSize....3095
IntervalCounter 3098
LogicalDiskStats....3100
MemByProcess 3103
MemUtil....3105
NetSession....3107
NetworkBusy....3108
PagingHigh....3109
PhysicalDiskStats 3110
PortHealth....3112
PrinterHealth 3113
PrinterQueue 3115
ProcessDown....3116
Processes....3117
ProcessUp 3118

RegistryChange 3120
RemoteServiceDown 3123
RemoteServiceDownLR 3125
Report_CPULoad 3127
Report_CPULoadSummary 3129
Report_CPUResource 3132
Report_CPUResourceSummary 3134
Report_CPUUsageofProcessesSummary 3137
Report_FilesOpen 3140
Report_LogicalDiskAvailSummary 3142
Report_LogicalDiskUsageSummary 3145
Report_MemoryUtilization 3148
Report_MemoryUtilizationSummary 3150
Report_NetworkBusy 3153
Report_PagingHigh 3155
Report_PhysicalDiskIO 3157
Report_PhysicalDiskQueueLength 3159
Report_PrinterHealth 3161
Report_Process 3163
Report_TopCPUProcs 3165
Report_TopMemoryProcs 3166
RunAwayProcesses 3167
ServerBusy 3169
ServerBytes 3170
ServerError 3171
ServerTimeout 3172
ServiceChange 3173
ServiceDown 3174
ServiceDownLR 3177
ServiceHung 3179
ServiceRemove 3181
SharedFiles 3182
SystemUpTime 3183
TopCpuProcs 3184
TopMemoryProcs 3185
TrustRelationship 3186
UnixRemoteProcessDown 3187

Chapter 54
NTAdmin Knowledge Scripts 3191
AddGroup 3193
AddGroupViaAD 3195
AddUser 3196
AddUserViaAD 3197
ChangePassword 3198
CheckServicePack 3199
CloseSharedFiles 3201
DeleteGroup 3202
DeleteUser 3203
FileCheck 3204
ModifyServiceConfig 3205

RegistrySet....3207
RestartService....3209
RunDOS....3211
SNMPSet....3213
SyncTime....3216
UnixAgentHealthProxy....3217

Chapter 55
OCS Knowledge Scripts 3219
ArchivedVoIPCallActivity....3220
ConferenceCallActivity....3223
CWAIMFailures....3226
CWAIMSessionActivity....3227
CWAServerStatus....3228
CWAUserSessionActivity....3229
CWAUserSessionFailures....3230
EdgeServerCallActivity....3231
EdgeServerCallFailures....3233
HealthCheck....3234
MCUStatus....3235
MediationServerCallActivity....3236
MediationServerCallFailures....3238
MediationServerHealth....3239
MediationServerUsage....3241
SessionCallActivity....3243
SessionCallFailures....3246
SystemUptime....3248
SystemUsage....3249

Chapter 56
Oracle Knowledge Scripts 3251
How Knowledge Scripts Access Oracle Databases....3253
AlertLog....3254
BGProc....3256
Block....3258
BlockingSessions....3260
Cache....3261
CallRate....3263
CallsPerTransaction....3264
ConfigDB....3265
ConsistentChangeRatio....3266
ContinuedRowRatio....3267
DatabaseDown....3268
DatafileSpace....3270
DiskSpaceAvail....3271
OpenCursors....3273
RecursiveToUserCallRatio....3275
RedoLogContention....3276
RedoLogSpaceWaitRatio....3277
Report_BackgroundProcess....3278

Report_CacheHitRatio....3281
Report_DatabaseAvailability....3284
Report_DatafileSpace....3286
Report_DiskSpaceAvailable....3289
Report_TablespaceAvailable....3292
Report_TransactionRate....3295
Report_UserLocks....3298
RollBackSegmentContention....3301
RowSourceRatio....3302
RunSql....3303
SegmentExtentAvail....3307
SortOverflowRatio....3309
SysStat....3310
TablespaceAvail....3312
TopCpuUsers....3314
TopIOUsers....3315
TopLockUsers....3316
TopMemoryUsers....3317
TransactionRate....3318
UserCallsPerParse....3319
UserRollbackRatio....3320
UserSessions....3321

Chapter 57
Oracle-RT Knowledge Scripts 3323
ADOQuery....3324
AdvancedADOQuery....3328
ODBCQuery....3333
Report_Oracle-RT....3336

Chapter 58
OracleUNIX Knowledge Scripts 3339
ActiveTransactions....3342
AlertLog....3344
BGProc....3346
Block....3348
BlockingSessions....3350
BufferBusyWaits....3351
Cache....3353
CallRate....3355
CallsPerTransaction....3356
ClusterInstanceDown....3357
ConsistentChangeRatio....3358
ContinuedRowRatio....3359
DatabaseConnect....3360
DatabaseDown....3361
DataFileSpace....3363
DataRatios....3364
DiskSpaceAvail....3367
FreeListWaits....3369

HealthCheck 3371
Listener 3374
Memory 3377
MostExecutedSQLStatements 3383
OpenCursors 3385
Performance 3387
RedoLog 3391
RedoLogContention 3394
RedoLogsNotArchived 3395
RedoLogSpaceWaitRatio 3397
RollbackSegmentContention 3398
RowSourceRatio 3399
RunSql 3400
ScheduledJobs 3403
SegmentExtentAvail 3404
SetMonitoringOptions 3407
SortOverflowRatio 3409
SysStat 3410
TablespaceAvail 3412
TopCpuUsers 3418
TopIOUsers 3420
TopLockUsers 3422
TopMemoryUsers 3423
TopResourceConsumingSQL 3425
Transaction 3427
TransactionRate 3431
UpdateInstances 3432
User 3434
UserCallsPerParse 3437
UserRollbackRatio 3438
UserSessions 3439

Chapter 59
PhoneQuality Knowledge Scripts 3441
AddCiscoPhone 3442
CiscoPhoneQuality 3444
RemovePhone 3447

Chapter 60
PowerShell Knowledge Scripts 3449
RunCommand 3450

Chapter 61
ReportAM Knowledge Scripts 3453
AgentMaintenance 3455
AggValueHistory 3456
ApplicationInfo 3459
AvgMaxMinValue 3460
AvgValueByDay 3462
AvgValueByHr 3464

AvgValueByMin 3466
Chart2HTML 3468
Compare24Hours 3469
Compare24HoursLD 3471
CompDeploy 3473
CompLic 3474
CompVersion 3476
CurrentDiskSpaceUsage 3477
DataStream 3480
DataSummary 3481
DeletedObjects 3485
DetailData 3486
DFSSummary 3488
EventArchiveSummary 3489
EventSeveritySummary 3491
EventStatisticsSummary 3492
EventSummary 3493
FRSSummary 3495
GeneralCounter 3496
GeneralMachineDown 3498
GroupPolicySummary 3500
Inventory 3501
JobInfo 3503
JobSummary 3505
LastDataPoint 3507
ModuleUsage 3509
NetworkInterface 3511
NTLogicalDisk 3512
NTPhysicalDisk 3513
PerfOverview 3514
PerfOverviewLD 3516
PlainDataInfo 3518
PrinterSummary 3520
SerLevAvailability 3521
SQLDBInfo 3523
SystemUpTime 3524
SystemUpTimePie 3526
WatchList 3528

Chapter 62
SharePoint Knowledge Scripts 3531
BytesTransfer 3533
ConnectionsInterval 3534
ContentManagementEventLog 3535
DBSpaceUtil 3536
GenericEventLog 3537
HealthCheck 3539
InfoPathEventLog 3541
IsolatedApps 3543
RecycleBinInfo 3544
Report_ServerUptime 3546

Report_SiteInfo 3549
Report_SiteUsage 3551
Report_WebPartInfo 3553
ServerUptime 3555
ServiceUptime 3556
SiteEventLog 3557
SiteInfo 3559
SiteUsage 3561
WebPagePerf 3563
WebPartInfo 3564

Chapter 63
Siemens ServerView Knowledge Scripts 3565
AdaptecLogicalDriveStatus 3567
AdaptecPhysicalDiskStatus 3568
AdaptecRAIDControllerStatus 3569
ArrayLogicalDriveStatus 3570
ArrayPhysicalDiskHardErrors 3571
ArrayPhysicalDiskMiscErrors 3572
ArrayPhysicalDiskParityErrors 3573
ArrayPhysicalDiskSoftErrors 3574
ArrayPhysicalDiskStatus 3575
CPU 3576
Fan 3577
HealthCheck 3578
IDEPhysicalDevice 3579
LSILogicalDriveHealth 3580
LSIPhysicalDeviceHealth 3581
MemoryModule 3583
NICError 3584
NICFail 3585
OverallCondition 3586
PowerSupply 3587
SCSIPhysicalDevice 3588
Temperature 3589
Voltage 3590

Chapter 64
Snmp Knowledge Scripts 3591
Customizing Snmp Knowledge Scripts 3592
AddMIBs 3595
DeviceReboot 3597
InterfaceState 3599
RemoveMIBs 3601
SNMPTrap_Async 3603
SyncGet 3605
SyncGetTable 3609
SyncPoll 3614
SyncPollTable 3617
SyncSet 3620

Discovery_Snmp 3622

Chapter 65
SNMPUNIX Knowledge Scripts **3625**
AddMIBs 3627
DeviceReboot 3629
InterfaceState 3631
RemoveMIBs 3633
SyncGet 3635
SyncGetTable 3639
SyncPoll 3643
SyncPollTable 3646
SyncSet 3650

Chapter 66
SQL Knowledge Scripts **3653**
Accessibility 3657
BackupJob 3659
Bcp 3661
BlockedProcesses 3663
CacheHitRatio 3664
ClusterOwner 3665
Connectivity 3666
CPUUtil 3667
DataGrowthRate 3668
DataSpace 3670
DBGrowthRate 3672
DBLocks 3674
DBMirroring 3676
DBMirrorStatus 3679
DbOption 3681
DBSpace 3684
DBStats 3687
ErrorLog 3690
ErrorLogEx 3692
LockUtil 3694
LogGrowthRate 3695
LoginFailures 3697
LogShipping 3699
LogSpace 3701
MemUtil 3703
MonitorDDL 3704
MonitorJobs 3706
NearFileMaxSize 3708
NearMaxConnect 3710
NearMaxLocks 3711
NetError 3712
ParseErrors 3713
ProcessingTime 3715
RepLatency 3717

Replication 3718
Report_Accessibility 3720
Report_CacheHitRatio 3722
Report_DatabaseDataSpace 3724
Report_DataSpaceAvailabilitySummary 3726
Report_DataSpaceUtilizationSummary 3729
Report_DBSpaceAvailabilitySummary 3732
Report_DBSpaceAvailable 3735
Report_DBSpaceUtilizationSummary 3737
Report_ErrorLogSummary 3740
Report_NearMaxConnect 3743
Report_NearMaxLocks 3745
Report_NetError 3747
Report_Replication 3749
Report_ReplicationLatency 3752
Report_SpaceAvailability 3754
Report_SpaceAvailabilitySummary 3756
Report_SpaceUtilizationSummary 3759
Report_To-Be-ReplicatedTransactions 3762
Report_TopCPUUsers 3764
Report_TopCPUUsersDetail 3766
Report_TopIOUsers 3768
Report_TopIOUsersDetail 3770
Report_TopLockUsers 3772
Report_TopLockUsersDetail 3774
Report_TopMemoryUsers 3776
Report_TopMemoryUsersDetail 3778
Report_TopResourceUsers 3780
Report_TransactionsReplicatedPerSec 3782
Report_UserConnections 3784
Report_UserConnectionsSummary 3786
Report_UserMaxConnections 3789
RepTransactions 3791
RepTranSec 3792
RunSql 3793
ServerDown 3797
ServerThroughput 3798
SPIDsMonitoring 3799
StoredProcRecompiles 3800
TopCPUUsers 3801
TopIOUsers 3803
TopLockUsers 3805
TopMemoryUsers 3807
TopResourceUsers 3809
UserConnections 3812
UserMaxConnection 3813

Chapter 67
SQL-RT Knowledge Scripts **3815**
ADODSNQuery 3816
ADOQuery 3820

AdvancedADOQuery 3824
ODBCDSNQuery 3829
ODBCQuery 3832
Report_SQL-RT 3835
Report_SQL-RT_DSN 3837

Chapter 68
UNIX Knowledge Scripts **3839**
Creating Filters with Regular Expressions 3842
AIXLparUtil 3844
ApplicationProcessMonitor 3846
AsciiLog 3848
CpuByProcess 3851
CpuLoaded 3852
CpuResources 3854
CpuUtil 3856
DNSConnectivity 3858
DNSHealth 3859
DNSReplication 3861
DynamicFileSystemSpace 3863
FailedLogon 3865
FileSystemSpace 3867
FileSystemSpaceLC 3869
GeneralCounter 3871
HTTPHealth 3873
LargeDir 3874
LogicalDiskBusy 3875
LogicalDiskIO 3876
LogicalDiskUtilization 3877
MemByProcess 3878
MemShortage 3879
MemUtil 3880
NetInterfacesCollision 3882
NetInterfacesConnectivity 3883
NetInterfacesDown 3884
NetInterfacesErrors 3885
NetInterfacesIO 3886
PagingHigh 3887
PhysicalDiskBusy 3888
PhysicalDiskIO 3889
PingMachine 3891
PortHealth 3893
PrinterQueue 3894
PrivilegedProcs 3895
ProcessDown 3896
Processes 3897
ProcessUp 3898
RemoteProcessDown 3899
Report_CPULoad 3903
Report_DiskUsageSummary 3905
Report_MemoryUtilization 3908

Report_NetInterfacesIO 3910
Report_SystemUpTime 3912
Report_TopMemoryProcs 3914
RunAwayProcs 3916
RunCommand 3917
SwapLow 3918
Syslog 3919
SystemUpTime 3921
TopCpuProcs 3922
TopMemoryProcs 3923
ZombieProcs 3925

Chapter 69
VMware VirtualCenter Knowledge Scripts 3927
Alarms 3929
Using the Alarms Script to Monitor ESX Hardware 3932
ClusterCPUusage 3934
ClusterMemUsage 3936
ClusterStatus 3939
Configuration 3941
ConfigureHostTraffic 3944
DatastoreUsage 3946
Events 3948
HostConnected 3952
HostCPUUsage 3954
HostDataStoreUsage 3957
HostDiskIO 3959
HostDiskTotalLatency 3961
HostMemoryUsage 3964
HostNetworkIO 3971
HWCorrectableMemCondition 3973
HWFanStatus(CPU) 3975
HWFanStatus(System) 3977
HWHPNICLost 3979
HWHPNICRestorScripted 3981
HWLogicalDiskStatus 3983
HWPhysicalDiskStatus 3985
HWPowerSupply 3987
HWThermalStatus 3989
ResourcePoolCPUusage 3991
ResourcePoolMemUsage 3993
ResourcePoolStatus 3995
ServiceHealthCheck 3997
Tasks 3999
VirtualCenterCPUUsage 4001
VirtualCenterMemoryUsage 4002
VirtualMachineInventory 4003
VmConnected 4005
VmCPUusage 4007
VmDiskIO 4011
VmDiskUsage 4013

VmMemoryUsage 4015
VmNetworkIO 4020
VmPowerStatus 4022
VmToolsStatus 4024
VirtualCenter_RPT_VCConfiguration 4026
VirtualCenter_RPT_VCCPUUsage 4028
VirtualCenter_RPT_VCHostDataStoreUsage 4031
VirtualCenter_RPT_VCMemoryUsage 4033
VirtualCenter_RPT_VCNetworkIO 4035
Recommended Knowledge Script Groups 4037

Chapter 70
VoIPQuality Knowledge Scripts 4039
CallPerf_G711a 4040
CallPerf_G711u 4044
CallPerf_G723.1-ACELP 4048
CallPerf_G723.1-MPMLQ 4052
CallPerf_G726 4056
CallPerf_G729 4060
CallPerf_G729A 4064
CiscoSAA_G711a 4068
CiscoSAA_G711u 4070
CiscoSAA_G723.1-ACELP 4072
CiscoSAA_G723.1-MPMLQ 4074
CiscoSAA_G726 4076
CiscoSAA_G729 4078
CiscoSAA_G729A 4080
Report_Configuration 4082
Report_GroupSummary 4083
Report_MOSAvailMatrix 4085
Report_MOSSummary 4087
Report_RvalueSummary 4089
Report_TimeDetail 4091
Report_VoIPQualitySummary 4093
Reviewing Call Performance Metrics 4095
Diagnosing VoIP Quality Problems 4097
Reviewing Quality of Service 4098

Chapter 71
WebLogicSvrUnix Knowledge Scripts 4101
Availability 4106
ClusterMessage 4107
ConnectorConnCurrent 4109
ConnectorConnRequests 4111
EntityEJBCache 4113
EntityEJBError 4115
EntityEJBPool 4116
EntityEJBTrans 4117
EntityEJBWait 4118
HealthCheck 4119

JDBCAvailableConnections 4121
JDBCClients 4123
JDBCConnections 4125
JDBCConnectionCapacity 4127
JDBCEnableSQLProfiling 4128
JDBCSQLMonitoring 4129
JDBCSQLMonitoringTopN 4131
JMS 4132
JMSConnectionsSessions 4134
JMSHealthState 4135
JMSPooledConnAvail 4136
JMSPooledConnError 4138
JMSPooledConnSession 4139
JMSPooledConnWait 4141
JMSServersBytesStored 4142
JMSServersDestinations 4144
JMSServersHealthState 4145
JMSServersMsgsStored 4146
JMSServersSessionPools 4148
JRockitGC 4149
JRockitThreads 4150
JTAActiveTrans 4151
JTACompletedTrans 4152
JTAHealthState 4154
JTATransRolledBack 4155
LogAccessLog 4156
LogAccessLogSetPath 4157
LogWebLogic 4158
LogWebLogicSetPath 4160
Memory 4161
MsgDrivenEJBError 4162
MsgDrivenEJBPool 4163
MsgDrivenEJBTrans 4164
MsgDrivenEJBWait 4165
NetIQAgent 4166
Report_HealthSummary 4167
Report_PerfSummary 4169
SecurityUserLockout 4171
ServerCPU 4173
ServerHealthState 4174
ServerJVMHeap 4175
ServerRequests 4176
ServerSecurity 4178
ServerSockets 4180
ServerState 4181
ServerUptime 4182
ServletExecTime 4183
StartAdminServer 4185
StartServer 4186
StartServerNodeMgr 4187
StatefulEJBCache 4188

StatefulEJBTrans....4190
StatefulEJBWait....4191
StatelessEJBError....4192
StatelessEJBPool....4193
StatelessEJBTrans....4194
StatelessEJBWait....4195
StopServer....4196
TransCateg....4197
TransCategRollBacks....4199
TransResHealthState....4201
TransResHeuristics....4202
TransResources....4204
WebAppSessions....4206

Chapter 72
Web-RT Knowledge Scripts 4207
AppManager ResponseTime for Web Version Compatibility....4209
CheckURL....4212
FTP....4220
NNTPConnect....4223
ReceiveInternetMail....4225
Report_Web-RT_Mail....4228
Report_Web-RT_Steps....4230
Report_Web-RT_URLCheck....4232
Report_Web-RT_Web....4234
SendAndReceiveInternetMail....4236
SendInternetMail....4240
SMTPConnect....4243
TakeDesktopOwnership....4245
URLCheck....4246
WebTransaction....4250

Chapter 73
WebSphereAppSrvUNIX Knowledge Scripts 4255
Availability....4260
DynamicCacheEviction....4261
DynamicCacheHits....4263
EJBActivation....4264
EJBMessageDelivery....4266
EJBMessageSession....4267
EJBMethodCalls....4269
EJBPersistence....4270
EJBPool....4272
HealthCheck....4274
J2CUsage....4276
J2CWaits....4277
JDBCDriver....4279
JDBCUsage....4280
JDBCWaits....4281
JVMGCStats....4283

JVMHeap 4284
JVMLocks 4285
JVMObjects 4286
JVMThreads 4287
NetIQAgent 4288
ORBInterceptor 4289
ORBRequests 4290
Report_HealthSummary 4291
RequestMetrics 4293
ServerCPU 4294
ServerScanLog 4295
ServletErrors 4296
ServletRequests 4297
SessionErrors 4298
SessionInvalid 4299
SessionLifetime 4300
SetRMFilters 4301
SetServerLogPath 4303
StartServer 4304
StopServer 4305
ThreadPoolUsage 4306
TransactionCommits 4307
TransactionDuration 4309
WebAppLoads 4310
WLMClientRequests 4311
WLMServerRequests 4312
WSGWRequests 4313

Chapter 74
WebSphereMQUNIX Knowledge Scripts 4315
ADMINClearLocalQueue 4316
ADMINQueueMgrStartStop 4317
ChannelStatus 4318
DynamicLocalQueueDepth 4320
LocalQueueDepth 4321
PingQueueManager 4322
ServerDown 4323
TestQueueManager 4324
WebSphereMQErrorLog 4325

Chapter 75
WIN2000 Knowledge Scripts 4329
ADDNSRegistrationEventLog 4331
DFSLinkDown 4333
DFSServiceDown 4335
DiskQuotaStatus 4336
DNSAXFRStat 4338
DNSDatabaseNodeMemory 4339
DNSDynaUpdateError 4340
DNSDynaUpdateStat 4341

DNSEventLog 4342
DNSRecursiveQuery 4344
DNSSecureUpdate 4345
DNSTotalQuery 4346
DNSWINSStat 4347
DNSZoneTransfer 4348
FrsBusy 4349
FrsEventLog 4350
FrsReplicaError 4352
FrsServiceDown 4353
GroupPolicyAddRemove 4354
GroupPolicyCount 4355
GroupPolicyLinkSnapshot 4356
GroupPolicyRefresh 4357
GroupPolicySnapshot 4358
IASServiceDown 4359
LSASSWatch 4360
MSIPackagesChange 4361
PrinterErrors 4362
PrinterEventLog 4363
PrinterQueue 4365
PrinterUtil 4366
RemoteStorageEventLog 4367
RemoteStorageServiceDown 4369
RSVPEventLog 4370
RSVPServiceDown 4372
SMTPEventLog 4373
SMTPQueues 4375
SMTPServiceDown 4376

Chapter 76
WIN2003 Knowledge Scripts **4377**
ActivationGracePeriod 4379
AUDownLoaded 4380
AUOptionChange 4381
AUServiceDown 4382
AUVerifyHotFix 4383
BITSJobProgress 4384
BITSJobsActive 4385
BITSJobsError 4386
BITSJobState 4387
BITSJobStats 4388
BITSServiceDown 4389
CLRConnectionPools 4390
CLRContention 4392
CLRExceptions 4394
CLRHeap 4396
CLRJit 4398
CLRMemProfile 4400
CLRNetworking 4402
CLRRemoting 4404

CLRThreads....4405
DCOMAppChange....4407
FaxActivity....4408
FaxEventLog....4410
FaxServiceDown....4412
FaxTotalFailed....4413
FaxTotalTime....4414
OpenSystemSlots....4415
PNPDeviceChange....4416
PNPDeviceErrors....4417
PrinterStuckJobs....4418
SRDiskPercent....4419
SREventLog....4421
SRLifeInterval....4423
SRPoints....4424
SRScheduledInterval....4425
SRServiceDown....4426

Chapter 77
Windows-RT Knowledge Scripts 4427
ChangeLocking....4428
ClosePlayer....4429
TakeDesktopOwnership....4430

Chapter 78
WMI Knowledge Scripts 4431
Configure....4432
EventConsumer....4433
LogSizes....4434
RepositoryUsage....4435
ResourceHigh....4436
RunWQL....4437
ServiceDown....4439
UserManager....4440
Discovery_WMI....4442

Chapter 79
WTS Knowledge Scripts 4443
LoggedOffSessions....4445
Messenger....4447
SessionsInfo....4449
SessionsLogoff....4450
SessionsReset....4451
SessionsTimeout....4452
SessionsTotalActive....4453
SessionsTotalBytes....4454
SessionsTotalDisconnected....4455
SessionsTotalErrors....4456
SessionsTotalFrames....4457
SessionsTotalInactive....4458

SessionsTotalProtocolHitRatio....4459
TopCpuProcs....4460
TopCPUSessions....4461
TopCpuUsers....4462
TopMemorySessions....4463
TopMemoryUsers....4464
UsersInfo....4465

About this Book and the Library

The NetIQ AppManager product (AppManager) is a comprehensive solution for managing, diagnosing, and analyzing performance, availability, and health for a broad spectrum of operating environments, applications, services, and server hardware.

AppManager provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager, administrative staff can monitor computer and application resources, check for potential problems, initiate responsive actions, automate routine tasks, and gather performance data for real-time and historical reporting and analysis.

Intended Audience

This guide provides information for individuals responsible for installing an AppManager module and monitoring specific applications with AppManager.

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

Provides complete information about AppManager pre-installation requirements and step-by-step installation procedures for all AppManager components.

User Guide for AppManager Control Center

Provides complete information about managing groups of computers, including running jobs, responding to events, creating reports, and working with Control Center. A separate guide is available for the AppManager Operator Console.

Administrator Guide for AppManager

Provides information about maintaining an AppManager management site, managing security, using scripts to handle AppManager tasks, and leveraging advanced configuration options.

Upgrade and Migration Guide for AppManager

Provides complete information about how to upgrade from a previous version of AppManager.

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

The AppManager library is available in Adobe Acrobat (PDF) format from the NetIQ Web site: www.netiq.com/support/am/extended/documentation/default.asp?version=AMDocumentation.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and CD-ROM titles • Variable names and values • Emphasized words
`Fixed Font`	• File and folder names • Commands and code examples • Text you must type • Text (output) displayed in the command-line interface
Brackets, such as *[value]*	• Optional parameters of a command
Braces, such as *{value}*	• Required parameters of a command
Logical OR, such as *value1*|*value2*	• Exclusive parameters. Choose one parameter.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measureable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

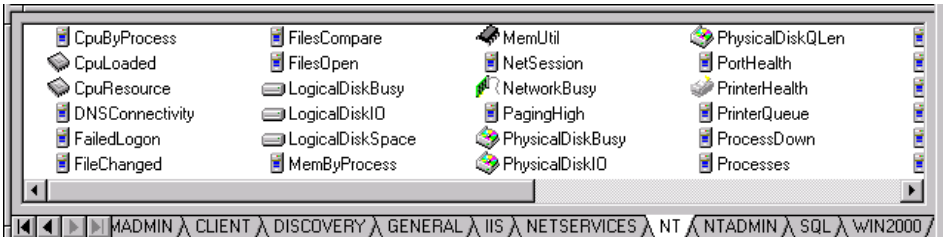
Chapter 1
Introduction to Knowledge Scripts

This topic provides an introduction to the Knowledge Scripts available in the NetIQ AppManager product and a brief review of how Knowledge Scripts are used to set up and run monitoring jobs. It also includes information about special privileges that are required to run some Knowledge Scripts.

Introduction to Knowledge Script Categories

Knowledge Scripts are grouped into categories and displayed under different tabs in the Knowledge Script pane in the Operator Console. Some Knowledge Script categories — such as AMAdmin, Discovery, General, and Action — are available to all users. The availability of additional Knowledge Scripts categories depends on the servers you are managing and the AppManager modules you have purchased and installed. For example, if you have licensed and installed AppManager for Microsoft Exchange 2007, and AppManager for Microsoft SQL Server, the Knowledge Script pane includes tabs for these Knowledge Script categories.

A typical set of the Knowledge Script categories for most users looks similar to this:



Understanding Resource Types and Type Checking

Each Knowledge Script is associated with one or more **resource object types**. The type determines which resource objects the Knowledge Script can be applied to. For example, it does not make sense to run a Knowledge Script that monitors Exchange mail on a SQL Server. Internally, AppManager handles the type checking to ensure that each Knowledge Script runs only on the types of resource objects that it can manage.

Folders and Objects

The resource types shipped with AppManager fall into two categories: **folders** and **objects**.

Folders

Used to group similar objects to simplify viewing. Folders can be opened (expanded) or closed (collapsed) to view the objects contained within them.

Objects

Individual resources that AppManager can monitor, such as disk drives or CPU resources.

As an example, the NT TreeView includes a Logical Disk folder icon. All of the logical disk icons underneath the folder, for example, `C:` or `D:`, represent individual logical disk partitions and are resource objects of the same type.

Icons Displayed for Matching Type

When a Knowledge Script is dragged into the TreeView and an object icon becomes a green dot, it means the Knowledge Script type matches the target object's type. If the icon is displayed with a right arrow, the Knowledge Script type matches the type of at least one of the object's children. If the icon has a left arrow, it means the Knowledge Script type matches the type of at least one of the object's parents.

If any of these icons is displayed, the Knowledge Script has found an appropriate target and can start a job. If a green icon is not displayed, the Knowledge Script does not match the object and the job cannot be started.

If a Knowledge Script is dropped on an appropriate object and an event is detected, the event indicator highlights the specific object icon where the problem was found in the TreeView pane. Any parent objects or folder icons also flash to alert you to the event, all the way to the top of the TreeView. So, even if an object is folded into its parent's icon, an indication of the event is always visible.

Understanding How Knowledge Scripts Work

When a Knowledge Script is dropped on a target, one or more jobs may be created and sent to the target computers being managed. If the Knowledge Script is dropped on a single computer, one job is created and sent to that computer. If the Knowledge Script is dropped at a higher point in the hierarchy, there may be multiple managed client computers and thus multiple jobs may be created.

Each job represents the associated Knowledge Script running on the target managed client computer by the AppManager agent. Once started, the Knowledge Script job continues to run according to its schedule. If an event is detected or data is collected, the managed client sends the data or event information to the management server. The management server then transfers the data or event information to the central AppManager repository (QDB). The AppManager repository stores the information in its database.

Most Knowledge Scripts monitor the performance and availability of your servers or diagnose problems in your environment. In addition to these standard operations, there are four special types of Knowledge Scripts that perform specialized tasks and function a little differently:

- Monitor-By-Proxy Knowledge Scripts
- Asynchronous Knowledge Scripts
- Local Configuration Knowledge Scripts
- Action Knowledge Scripts

Monitor-By-Proxy Knowledge Scripts

Most Knowledge Scripts perform their tasks on the local computer on which you run them. However, some Knowledge Scripts run on one computer but allow you to specify one or more remote computers on which they are to perform their tasks.

Additionally, the tasks that are performed on the remote computer do **not** require the AppManager agent to present on the remote computer. For example, the NT_RemoteServiceDown Knowledge Script monitors services on other computers and General_MachineDown monitors whether a computer can communicate with remote computers.

AppManager provides the following proxy Knowledge Scripts:

- AnalyticsAlarm_ProcessClearEvents
- AnalyticsAlarm_ProcessTrustedAlarms
- General_MachineDown
- General_MachineDownLR
- General_PingMachine
- NT_RemoteServiceDown
- NT_RemoteServiceDownLR

Note that with the exception of General_MachineDown, which is configured to browse the repository for the list of remote computers you want, these Knowledge Scripts display event information in the Operator Console even if the remote computer is in maintenance mode.

When providing a list of Windows computers, you can specify computers that are not currently in the TreeView pane of the Operator Console. Note that if a remote computer is not in the TreeView pane of the Operator Console and this Knowledge Script raises an event on that computer, a server group named **AppManager Proxy Events** is automatically created in the **Master** view. From this group, you can view, acknowledge, close, and delete all events on the computer. To discover resources and run monitoring jobs on the computer, you must delete the computer from the **AppManager Proxy Events** server group, then manually add the computer to the TreeView. If necessary, stop any proxy jobs that are monitoring the remote computer so you can add it to the TreeView.

When configuring an action for monitoring-by-proxy Knowledge Scripts, you should configure the Location to initiate the action on the MS (to run on the management server) or on a Proxy (to run on a particular managed client computer).

If you instead configure an action to run on the managed client (MC), when a remotely monitored computer is placed into machine maintenance mode (from the Operator Console) or scheduled maintenance mode (using the AMAdmin_SchedMaint Knowledge Script), any event conditions detected on the remote computer are ignored but the action is not disabled; in this case, an action will be run but there will be no event information in the Events tab of the Operator Console.

Asynchronous Knowledge Scripts

Most Knowledge Scripts run once or on a schedule you specify. However, there are some Knowledge Scripts that run asynchronously whenever a certain event occurs. For example, Async_FilesChanged monitors one or more files for changes and raises an event when a change occurs. Instead of running a periodic check at a set interval, these Knowledge Scripts are always "active" and alert you whenever a new event occurs.

Local Configuration Knowledge Scripts

Most Knowledge Scripts run in accordance with parameters you set when you run the Knowledge Script. However, there are six Knowledge Scripts that get some parameter values from the local repository on the computer on which you run them. These parameter values are set by configuration Knowledge Scripts that you run in advance.

The combination of configuration Knowledge Scripts and local-repository Knowledge Scripts enables you to configure a group of computers differently as a one-time operation, then run the local-repository Knowledge Scripts as part of a monitoring policy on the whole group. The local-repository Knowledge Scripts behave differently on each computer in the group because they use the local parameter values instead of their own.

To understand how this works, consider the following configuration and local-repository Knowledge Script pairs:

NT_ConfigLogicalDisks

Specifies the logical drives and thresholds to monitor. These parameters are then used locally by the **NT_LogicalDiskSpaceLR** and the **NT_LogicalDiskIOLR** local-repository Knowledge Scripts.

NT_ConfigServiceDown

Specifies the services to monitor. This parameter is then used locally by the **NT_ServiceDown** local-repository Knowledge Script.

The other configuration Knowledge Scripts function in a similar way.

There are also AMAdmin Knowledge Scripts you can use to:

- View local repository (LR) configuration information: LRReadParameters
- Remove local repository (LR) configuration information: LRRemoveParameters
- Store local repository (LR) configuration information: LRWriteParameters

Action Knowledge Scripts

Most Knowledge Scripts run when you drag and drop them on a computer or a resource object in the TreeView. However, you never start Action Knowledge Scripts by dragging and dropping them onto an object. Instead, Action Knowledge Scripts are started indirectly by other types of Knowledge Scripts in response to events raised by those scripts.

To specify one or more Action Knowledge Scripts to run, use the Action tab of the script Properties dialog box when you set the properties for any other type of Knowledge Script.

Setting Knowledge Script Properties

Each Knowledge Script has properties you can modify. The Knowledge Script Properties dialog box is displayed when you:

- Double-click a Knowledge Script in the Knowledge Script pane of the Operator Console
- Select a Knowledge Script in the Control Center console
- Drag a Knowledge Script to the TreeView pane of the Operator Console

- Double-click a Knowledge Script job entry in the Jobs list

For most Knowledge Scripts, the Knowledge Script Properties dialog box lets you set the following:

Schedule

Every Knowledge Script has a default interval, for example, every five minutes, once a day, or only once. You can modify the schedule to use a different interval, to start and stop at specific times, or to run only once.

Values

Most Knowledge Scripts require some parameters to be set. The parameters vary depending on the purpose of each script, but the most common parameters allow you to raise events, set thresholds that will raise events, collect data for graphing and capacity planning, and set event severity levels. Default values are provided for most parameters, but you can easily modify them as needed.

Actions

These are the optional actions that a Knowledge Script can initiate if an event is detected. You can choose to raise one or more actions when an event is raised.

Objects

This tab lists the objects against which you have indicated you want the Knowledge Script to run. You can use this list to modify the objects to run against.

Advanced

This tab is used to set advanced job properties. It allows you to indicate whether you want duplicate events or the job collapsed into a single event, and the number of consecutive event occurrences to allow before raising an event in the Operator Console.

Viewing Job Results

Knowledge Scripts display the results of your jobs in several ways. What you see depends on whether your job is set for events, data collection, or both, or if the script runs into an error. For example, if a job is used to raise events, you see blinking icons in the Operator Console; if a job is used to collect data, you may view the results in a graph; if a job runs into an error, an Error status is displayed for the job under the Jobs tab.

Viewing Detailed Information

When events are generated as the result of a job, you can often get additional details about what happened by double-clicking the child event entry under the Events tab in the List pane. For example, the detail message for a TopCpuProcs Knowledge Script job includes a list of processes that consume the most CPU time. Depending on the Knowledge Script and the event, the detail message may include quite a lot of additional information about the problem found and how to correct it.

Similarly, when you run a Knowledge Script to collect data, the Knowledge Script creates one or more data streams that can be graphed. Once a data stream is graphed, double-clicking a data point on the graph displays a Graph Data Details dialog box that shows additional information about the data point selected.

Using Filters to Fine-Tune Searches

Some Knowledge Scripts search Windows event logs or other log files for specific types of information. In many cases, you can use a **filter** to fine-tune the types of information the Knowledge Script searches for. In the Values tab of the Knowledge Script Properties dialog box, a **Filter** parameter lets you specify a string of characters to look for.

How Filtering Works

Filtering is done through the combination of parameter values you set using partial string matching, without regard to case. For example, if you enter `Log` in the *Event Description* parameter, the filtering mechanism will include entries such as "The parameters specified for **log**ging are too long," and "The server failed to create a **log** context." For each filter you can specify the strings to include, exclude, or both.

Specifying Filters that Include Information

A filter searches for any entry that wholly or partially matches the search string that you specify. For example, for an **Event Description Filter** or **Filter the Event Description field** parameter (the wording may vary depending on the Knowledge Script), you might specify a search string of "MSExchange" or "Exchange" (the quotes aren't needed in the parameter field):



If this is the only filter you have specified, the Knowledge Script searches only the Description field in the log file and returns entries that include the string, such as MSExchangeAdmin, MSExchangeDSExp, MSExchangeDSImp, and MSExchangeSetup.

If you want the Knowledge Script to return all entries without filtering them, leave the filter parameter blank for text fields (such as a Computer Name), and specify 0 for fields containing numbers (for example, in the case of an Event ID).

General Rules for Matching Strings

For most filters, you can type any part of the text string you want to match and filtering is not case sensitive. If you specify a filter of "error" or "eRr", the Knowledge Script ignores capitalization and finds entries such as sys_err, error, Error, ERROR, and so on.

For example, you can filter the Source field in the Application event log for entries that have MSSQLServer as their source, by typing any part of that string for the Event Source filter (`ms`, `sql`, or `sqls` would all be valid search strings to find MSSQLServer):

Note
The exception to this rule is the Event ID filter, which requires a number. For the *Filter the Event ID field for* parameter, only exact matches are returned.

The filter string you specify can include spaces, underscores, and periods. For example, you can specify a very complete Event Description filter, such as "DHCP IP address lease 10.1.10.157".

Filters do not, however, recognize regular expressions or wild cards. If you specify a filter of "*32.dll" or "?32.dll" the Knowledge Script will search for entries that include the exact string you specified (`*32.dll` or `?32.dll`). Because file names cannot contain the * or ? characters, no entries will be returned.

Specifying Multiple Search Strings

You can specify multiple search strings for any filter by separating the strings with a comma and no extra spaces. For example to search the Event Description field for any of the following entries, enter:

```
DHCP IP address lease 10.1.10.157,20,error
```

In most cases, you can also combine filters to narrow matching entries further. For example, if you want to look for a specific event description occurring on any one of several specific computer names, you might set both the Event Description Filter and the Computer Filter:



If you specify multiple filters, the Knowledge Script searches only for entries that satisfy all of the search strings. For example, if you enter "1234" for the Event ID filter and "Fred" for the User field filter, the script only finds log entries that satisfy both filters.

Specifying Filters that Exclude Information

The information that you exclude from a search follows the same rules for including information: the Knowledge Script searches for partial matches and is not case-sensitive. The only difference is the format of the search string itself.

A single search string can specify information both to include and exclude. Separate the included and excluded strings with a colon (`included:excluded`). The string to the left of the colon is included in the search; the string to the right of the colon is excluded from the search. Separate multiple include or exclude entries with commas. For example, to search the Source field for entries that include the string "perf" and do not include the string "mon" or "lib", specify this filter parameter: `perf:mon,lib`.

Similarly, to search the **Computer** field for all Sales computers except those with Corp00 and HQ in their name, specify this filter parameter, `sales:corp00,HQ`.

The filter finds computer names such as NwSales, SalesEuro, and Corp02Sales but not NwSalesHQ or Corp00Sales.

To specify only the information to exclude, start the search string with a colon. For example, to search the Description field for all entries except those containing ODBC and RPC, specify this filter parameter: `:ODBC,RPC`.

If you are searching only for included strings, the colon is not necessary. For example, to search the Category field for entries with the string "SQL", specify this filter parameter: `SQL`.

Creating Filters with Regular Expressions

Some Knowledge Scripts enable you to use regular expressions to define include and exclude filters for pattern-matching against the text being evaluated. Depending on the Knowledge Script you are working with, you may be able to use regular expression include and exclude filters when you are setting job properties or you may be able to maintain your search criteria independent of the Knowledge Script parameters in a separate filter file. You may also be able to use regular expression modifiers to further refine your filtering.

For example, if your **include filter** looks like this `replic.*` and you specify the modifier `i` to make the search case-insensitive, the regular expression contains the wildcard (`.`) and repeat (`*`) special characters, indicating you want to find strings that start with `replic` followed by any string of characters. Messages containing either `replication` or `replicated` are captured.

The format is the same for the exclude filter. For example, to find log entries that do not start with the string `success`, the exclude filter might look like this:

```
^success.*
```

If you are only searching for included strings, you can leave the exclude filter blank. If you want to retrieve all messages in the log in a given interval, you can specify `.*` for the include filter and leave the exclude filter blank.

Using Special Characters

The following special characters can be used in regular expressions:

Use This Character	For This Purpose
.	Wildcard for any one character
*	Repeat zero or more occurrences
^	Beginning of the line
\$	End of the line
\	Escape the next meta-character
|	Alternate matches
[ ]	Any character in the class set. You can specify individual characters or ranges.
( )	Grouping characters. For example, you can specify (a|b|c) to indicate a match with a, or b, or c.
+	Quantifier indicating one or more occurrences
?	Quantifier indicating zero or one occurrence
{*n*}	Quantifier indicating exactly *n* occurrence
\w	A word character (alphanumeric plus _)
\s	A white-space character
\d	A digit character

Using Regular Expression Modifiers

In addition to the special characters you can use in creating the regular expression, there are a number of modifiers that can be used to modify how pattern-matching is handled. For additional information about writing regular expressions, see your Perl documentation or other regular expression resources. Valid modifiers include:

Modifier	Description
c	Complements the search list
g	Matches globally as many times as possible
i	Makes the search case-insensitive
m	Treats the string as multiple lines
o	Interpolates variables only once

Modifier	Description
s	Treats the regular expression string as a single long line
x	Allows for regular expression extensions

Running Knowledge Scripts that Require Special Privileges

AppManager agent services can run either as the `LocalSystem` account or as a valid user account that you designate. By default, the two agent services are installed to run using the Windows `Local System` account, and in most cases, this account is sufficient for running a wide range of Knowledge Script jobs.

Some Knowledge Scripts, however, require the AppManager agent services to run using special account permissions or privileges to get information from a managed client or perform certain tasks. When the Update Definition in User Variables. agent runs under a user account, that account is typically called the **service account**.

A few Knowledge Scripts and managed objects require the AppManager agent services to run using a Windows login account that has Administrator privileges for the domain, that is, the account must be a member of **Domain Admins** and not just an Administrator for the local computer. It is the Domain Admins privilege that enables the Knowledge Scripts to read certain Performance Monitor counters, access protected files, or perform restricted actions such as creating directories and copying files on remote computers.

Other Knowledge Scripts have other account requirements. For example, some Exchange Knowledge Scripts require Exchange Admin permissions.

Review the *Management Guide* for each application you plan to monitor before you install agents on those servers. The management guides, which are included in application-specific folders under the `\Documentation\Management Guides` folder of the AppManager installation kit, provide lists of Knowledge Scripts that require special privileges and also contain instructions for changing the account under which the agent services are running.

Setting Up a Service Account

You can use an existing account or create a new account specifically for the agent services to use. To set the service account:

1. Use the Windows **Computer Management** tool or Windows 2000 **Active Directory** to set up or find an account with the appropriate privileges. For example, check that the user account is a member of the Domain Admins group.
2. Open the **Services** Control Panel and select the NetIQ AppManager Client Resource Monitor service.
3. Click **Stop** and wait for the service to stop.
4. On the Log On tab, click **This account**, then provide the user account and password you identified in Step 1.
5. On the General tab, click **Start** to restart the service.
6. Repeat Step 2 through Step 6 for the NetIQ AppManager Client Communication Manager service.

Running Administrator-Only Knowledge Scripts

Some Knowledge Scripts perform AppManager administrative tasks or operations that should be restricted to a limited number of users. To control access to these Knowledge Scripts, the scripts are only made available to users who are assigned to the Administrator role through Security Manager.

Most of the administrative Knowledge Scripts are in the Action, AMAdmin, and NTAdmin categories, and by default these Knowledge Scripts are designated as being for administrators only. You can, however, modify the administrator-only setting for any Knowledge Script through an option in the Developer's Console.

For more information about modifying Knowledge Scripts, see *Developing Custom Knowledge Scripts* for AppManager. For information about assigning users to security roles, see the Security Manager Help or the *Administrator Guide*.

Getting Online Help for Knowledge Scripts

To get Help for any Knowledge Script:

- Highlight the Knowledge Script in the Knowledge Script pane in the Operator Console and press **F1**.
- Select **Help Topics** from the Help menu and use Index or Find to look for the Knowledge Script you are interested in.
- Click the **Help** button while viewing the Values tab in the Knowledge Script Properties dialog box.

Online help is not provided for contributed, unsupported, or custom Knowledge Scripts.

Chapter 2
Action Knowledge Scripts

The Action category provides Knowledge Scripts to perform corrective or responsive actions when events are raised. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AddComputerToServerGroup	Adds a CallManager to a CallManager cluster based on its Publisher.
Diagnose	Triggers AppManager Diagnostic Console to run a diagnosis of the target computer.
DiagnoseNortelIPT	Triggers NetIQ Vivinet Diagnostics to run a diagnosis of VoIP quality in a Nortel CS1000 IP Telephony environment.
DiagnoseVoIPQuality	Triggers NetIQ Vivinet Diagnostics to run a diagnosis of voice quality between two phones or two endpoints.
DominoCommand	Issues a Domino command to a Domino server.
DosCommand	Runs a non-interactive DOS command.
DumpTran	Dumps or truncates the SQL Server transaction log.
ExtendedSNMPTrap	Sends an extended SNMP trap message to a specified list of computers.
IISContinueSite	Continues a paused Internet Information Services (IIS) site.
IISPauseSite	Pauses an IIS site.
IISRestartServer	Restarts an IIS server.
IISRestartSite	Restarts an IIS site.
MapiMail	Sends mail to one or more e-mail users.
Messenger	Sends a Messenger service message that contains AppManager event information to a specified computer.
NetAppFilerDoSnapMirror	Opens a Telnet session on the specified Network Appliance filer and issues a snapmirror command.
NetAppFilerIssueCommand	Opens a Telnet session on the specified Network Appliance filer and issues a non-interactive maintenance command.
NetAppFilerReboot	Opens a Telnet session into a specified Network Appliance filer and issues a reboot command.
NotesMail	Sends mail to one or more Lotus Domino/Notes e-mail users.
NTEventLog	Writes an event to the Windows Event Log.
Page	Sends a paging call to one or more recipients in response to an event.
RebootSystem	Shuts down and restarts a computer when an event is raised.

Knowledge Script	What It Does
RestartServices	Stops and restarts Windows services.
RunDiscoveryCiscoCallMgr	Used with CiscoCallMgr_CCM_RoleStatus to rediscover resources that move when a CallManager role changes.
RunDiscoveryNetworkDevice	Used with NetworkDevice_Device_Uptime to rediscover devices that reboot during monitoring.
RunKS	Runs up to three other Knowledge Scripts.
RunPhoneInventory	Used with CiscoCallMgr_LossOfHardwarePhones to produce a phone inventory on the associated Publisher.
RunPowerShell	Runs a non-interactive Windows PowerShell command.
RunSql	Runs SQL statements or stored procedures.
SendReportToPrinter	Sends a report to the printer that is the default for the managed client on which the Report agent is running.
SMTPMail	Sends mail using SMTP to one or more users.
SMTPMailRpt	Sends the first page of a report to a list of recipients.
SNMPTrap	Sends an extended SNMP trap to one or more computers.
StartServices	Starts specified Windows services.
StopServices	Stops specified Windows services.
Traceroute	Collects exception traceroute data between a specified source and target location in response to an event in a separate Knowledge Script.
TracerouteNetworks-RT	Collects exception traceroute data between a specified source and target location in response to an event in a separate Networks-RT Knowledge Script.
UpdateEventStatus	Provides AppManager event status details from one or more specified computers.
UXCommand	Runs a non-interactive UNIX command in response to an event.
WriteMsgToFile	Writes AppManager event information to a specified file.

AddComputerToServerGroup

Use this Knowledge Script to add a Cisco CallManager server to a CallManager cluster based on its Publisher. This script raises an event if the job is successful.

Note
Run this script only on a management server computer. Select **MS** (management server) as the Location on the Action tab of the Properties dialog box.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for success?	Set to **y** to raise an event when the process is successful.
Event level for success	Set the severity level, from 1 to 40, to indicate the importance of an event in which a CallManager servers is successfully added to a cluster.

Diagnose

Run this Knowledge Script to trigger AppManager Diagnostic Console to diagnose a problem on a *target* computer that has raised an event. The diagnosis is driven from the *console* computer specified in the **Location** field on the **Action** tab.

Notes

- This script requires AppManager Diagnostic Console 2.1 or later on the console computer and Diagnostic Console 2.0 or later on the target computer.
- Run this script only on a management server or proxy target computer. Select the **MS** (management server) or **Proxy** location on the Action tab of the Properties dialog box.

When launched, Action_Diagnose performs the following steps:

- Verifies that Diagnostic Console 2.1 or later is installed. If Diagnostic Console 2.1 or later is not installed, this script raises an event indicating that the diagnosis cannot be performed.
- Determines whether Action_Diagnose is already running on the console computer. If a diagnosis is already running, Action_Diagnosis raises an event indicating that a diagnosis is in progress. Only one instance of Action_Diagnose can be running at any given time.
- Invokes Diagnostic Console to perform the diagnosis and generate an `.html` diagnostic report. Diagnostic Console collects Windows, Exchange, or Active Directory data based on the configuration of the target computer.

  Note
  The target computer must have Diagnostic Console version 2.1 or later installed in order for Active Directory data to be collected. Windows and Exchange data can be collected with Diagnostic Console version 2.0 or later.

- Generates a report using the *Output folder prefix* and *Use Report Agent settings* parameters, or the *Full path to root of output folders* parameter if you are not using the Report agent.
- Upon completion of the diagnosis, raises an event that contains the results of the diagnosis. An event for a successful diagnosis will contain either a URL to the `default.htm` file (if *Use Report Agent settings* is set to **y**) or the computer name and full path of the location of the output files. An event for an unsuccessful diagnosis contains an error message explaining why the diagnosis was unsuccessful.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Length of time to run diagnosis	Enter the amount of time that you want a Diagnosis to run. The default is 300 seconds. The maximum allowable run time is 900 seconds; a longer run time will produce more data than reports can generate in a timely fashion. The minimum allowable run time is 60 seconds; a shorter run time is not enough for the agent to collect data and send it to the repository.
SQL Login Name	Enter the SQL user name required for access to the Appmanager repository when collecting Exchange and Active Directory data. Leave this parameter blank to use NT Authentication for accessing the repository.

Parameter	How to Set It
SQL password	Enter the SQL password required for access to the AppManager repository when collecting Exchange and Active Directory data.
Output folder prefix	Enter a prefix for the output folder that is generated by the diagnosis. The output folder then uses this prefix in the following naming convention: *Prefix_ComputerName_DateTime*. The default prefix is `Diag`. **Note** The `ComputerName` is the name of the computer being diagnosed.
Use Report Agent settings?	Set to **y** to specify that the Diagnostic results should be integrated into the AppManager Web management server (the Report Binder). The default is y.
Full path to root of output folders	Enter the full path to the root of where the output folders will be created. **Note** This parameter is ignored if **Use Report Agent settings** is enabled.
Event severity when …	Enter a severity level, between 1 and 40, to indicate the importance of the following events: • error. Raises an event when the diagnosis does not complete successfully. The default is 15. • successful. Raises an event when the diagnosis completes successfully. The default is 35.

DiagnoseNortelIPT

Run this Knowledge Script in your Nortel Communication Server 1000 IP Telephony environment to trigger NetIQ Vivinet Diagnostics to diagnose a call quality problem between two Nortel IP phones.

Configure this Action on the NortelCS_Alarms Knowledge Script. A Diagnosis is triggered when the Alarms script raises events for the following QoS alarms (SNMP traps): QOS0022, QOS0024, QOS0026, QOS0028, QOS0030, QOS0032, and QOS0034. The Diagnosis makes use of the RTCP-XT statistics included in the SNMP trap.

You must run this Action on a computer where Vivinet Diagnostics 2.0 (or later) is installed. In addition, you must have already configured Vivinet Diagnostics with the security information for accessing the Call and Signaling Servers. For more information, see the *User Guide for Vivinet Diagnostics*.

Only one Diagnosis can run at any time. If a second Action is triggered while a Diagnosis is already in progress, the second Action will complete, but indicate that it could not run the Diagnosis because another was already in progress. To see the status of the Action for any event, click the **Action** tab of the event.

When the Diagnosis has completed, the Action Knowledge Script raises an event that identifies the location of the Vivinet Diagnostics `.dgv` file, which contains the results of the Diagnosis. In addition, if the Web management server and Report agent are installed on the computer that is running the Action, you can enable the **Use Report Agent settings** parameter, which integrates the Diagnosis results with other reports generated by the Report agent. The results are then easily accessible from the Web management server Report Binder and from the Operator Console's **Extensions > Report Viewer** function.

Tip

To allow this script to trigger a Diagnosis with Vivinet Diagnostics whenever a problem occurs, you need to disable or modify the "event collapsing" feature on the NortelCS_Alarms script. Event collapsing allows AppManager to suppress, or collapse, what it considers to be duplicate events. However, you will probably want Vivinet Diagnostics to diagnose a problem each time one occurs, even if it occurs between the same two targets. And you cannot do that if AppManager has collapsed all call quality events between the same targets into one event. Use the Advanced tab of the NortelCS_Alarms script to disable event collapsing, or at least to modify the 20-minute collapsing interval.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Output folder prefix	Enter a prefix for the output folder that is generated by the Diagnosis. The output folder then uses this prefix in the following naming convention: *Prefix_JobID_Phone1_Phone2_DateTime*. The default prefix is `Diag`. `Phone1` and `Phone2` are the IP addresses of the two Nortel phones being diagnosed. The `ComputerName` is the name of the computer being diagnosed.
Use Report Agent settings?	If enabled, the diagnostic results are integrated into the AppManager Web management server (the Report Binder). The default is y.

Parameter	How to Set It
Full path to root of output folders	Enter the full local or UNC path to the root of the directory in which you want to create the output folders. Make sure that the `NetIQmc` service (NetIQ AppManager Client Resource Monitor) is configured to run as a user that has access to the UNC path. The default setting of "local system" does not have access to the UNC path. Without access to the path, Vivinet Diagnostics will not be able to save a Diagnosis to the output folder. **Note** This parameter is ignored if **Use Report Agent settings** is set to y.
Event Notification	
Severity when diagnosis successful	Enter a severity level, between 1 and 40, to indicate the importance of an event that is raised when the Diagnosis completes successfully. The default is 35.
Severity when error encountered	Enter a severity level, between 1 and 40, to indicate the importance of an event that is raised when an error prevents the Diagnosis from completing successfully. The default is 15.

DiagnoseVoIPQuality

Use this Action Knowledge Script to trigger NetIQ Vivinet Diagnostics to run a Diagnosis of voice quality between two phones or two endpoints. A Diagnosis is performed when a threshold is exceeded when you run any of the following Knowledge Scripts:

- **AvayaCM_CallQuality**. Vivinet Diagnostics can diagnose the problem when average MOS, average R-Value, average jitter, average latency, and average packet loss fall below or exceed their thresholds.
- **AvayaCM_PhoneQuality**. Vivinet Diagnostics can diagnose the problem when MOS, R-Value, jitter, latency, and packet loss fall below or exceed their thresholds during the data collection interval.
- **CiscoCallMgr_CallQuality**. Vivinet Diagnostics can diagnose the problem when jitter, latency, and percentage of lost data exceed their thresholds.
- **CiscoCallMgr_CallFailures**. Vivinet Diagnostics can diagnose the problem when the number of failed calls exceeds its threshold.
- **NortelCS2x_CallQuality**. Vivinet Diagnostics can diagnose the problem when end-of-call values for MOS and R-value fall below their thresholds, and when end-of-call values for jitter, latency, and packet loss exceed their thresholds.
- **NortelCS2x_PhoneQuality**. Vivinet Diagnostics can diagnose the problem when mid-call values for MOS and R-value fall below their thresholds, and when mid-call values for jitter, latency, and packet loss exceed their thresholds.
- **PhoneQuality_CiscoPhoneQuality**. Vivinet Diagnostics can diagnose the problem when the values for listening MOS and listening R-value fall below their thresholds, and when the values for average jitter, maximum jitter, and packet loss exceed their thresholds.
- **VoIPQuality_CallPerf_<***name of script***>**. Vivinet Diagnostics can diagnose the problem when MOS, R-factor, delay, jitter buffer loss, and percentage of lost data exceed their thresholds.

Note

This script is supported only when Vivinet Diagnostics 1.1 or later is installed. In addition, this script does not work when triggered by Knowledge Scripts other than those listed above.

When launched, Action_DiagnoseVoIPQuality performs the following steps:

- Verifies that Vivinet Diagnostics 1.1 or later is installed. If Vivinet Diagnostics 1.1 or later is not installed, this script raises an event indicating that Vivinet Diagnostics 1.1 is required.
- Verifies that you have elected to run this Action Knowledge Script based on an event raised by the running of an applicable script. If you choose to initiate this script based on some other Knowledge Script, this Action script raises an event indicating that the Action script cannot invoke Vivinet Diagnostics from the <*script name*> Knowledge Script.
- Determines the number of Diagnoses that need to be performed based on the parameters that you set in the above-mentioned scripts, as well as the thresholds that were reached or exceeded.
- Invokes Vivinet Diagnostics to perform the Diagnosis and generate an `.html` diagnostic report.
- If *Use Report Agent settings?* is disabled, generates a `default.rptIndex.xml` file and a small `default.htm` file that contains hyperlinks to the `.dgv` file and the Vivinet Diagnostic report.
- Upon completion of the Diagnosis, raises an event that contains the results of the Diagnosis. An event for a successful Diagnosis contains either a URL to the `default.htm` file (if *Use Report Agent settings?* is enabled) or the name of the computer and full directory path to the output files. An event for an unsuccessful Diagnosis contains an error message explaining why the Diagnosis was unsuccessful.

For a more in-depth discussion of the integration of Vivinet Diagnostics and AppManager, see the *User Guide for Vivinet Diagnostics*.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event severity when error	Set the severity level, between 1 and 40, to indicate the importance of an event in which a diagnosis does not complete successfully. The default is 15.
Event severity when successful	Set the severity level, between 1 and 40, to indicate the importance of an event in which a diagnosis completes successfully. The default is 35.
Output folder prefix	Enter a prefix for the output folder that is created by the Diagnosis. The output folder then uses this prefix in its naming convention as follows: *Prefix_JobID_ComputerName_DateTime*. **Note** The *ComputerName* is the name of the CallManager computer or talker/listener computer. If a single event triggers multiple Diagnoses, a sequence number (0, 1, 2, 3, 4) is appended to the output folder name. The output folder contains the `.dgv` file, the diagnostic `.html` report file, and, if integrated with the report-enabled agent, a `default.rptIndex.xml` file, and a `default.htm` file that contains hyperlinks to both the `.dgv` file and the diagnostic `.html` report.
Use Report Agent settings?	Select **Yes** to integrate the Diagnostics results into the AppManager Web management server (the Report Binder). The default is Yes.
Full path to root of output folders	Provide the full path to the root of where the output folders will be created. **Note** Ignore this parameter if *Use Report Agent settings?* is set to **Yes**.
Maximum diagnoses	Specify a number between 1 and 5 to indicate the maximum number of Diagnoses that can be triggered by a single event. **Note** This parameter is applicable only for events generated by the CiscoCallMgr_CallQuality and CiscoCallMgr_CallFailures scripts, where one event may identify multiple pairs of phones that indicate a problem.

DominoCommand

Use this Knowledge Script to issue a Domino command to a Domino Server. This script can enable you to run a Domino command as a corrective action in response to an event. For example, the Knowledge Script Domino_LogSniff monitors the Notes log database for specific messages or search strings. If you locate corruption in a database by running Domino_LogSniff, you can set that Knowledge Script to run the Action_DominoCommand Knowledge Script with the corrective Domino command or Domino agent you specify. The Domino command `Fixup`, for example, locates and repairs corrupted databases.

DominoCommand raises an event when the command is completed. The event message indicates whether or not the command was successful, and provides an explanation if the command fails.

Note
This Action can run only on the managed computer as a Managed Client Action. Select **MC** (Managed Client) on the Action tab of the Properties dialog box when enabling this Action.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Command	Specify the Domino command to be executed, using Domino command delimiters. For example, the default command, `0|#show task`, includes the following elements: • the partition number of the Domino server to which the command is being sent. If the computer contains only one instance of a Domino server, enter 0 • the vertical bar, | • the pound sign, # • the command, `show task` Domino commands must follow this format.

DosCommand

Use this Knowledge Script to run a non-interactive DOS command when an event is raised. For example, use this script to run a batch command for virus scanning, disk backup, or logging an entry in a trouble-ticket system.

You can include arguments in the command string. This script can also test your command-line syntax.

Use this Knowledge Script to create a script file that contains a series of commands to diagnose or correct problems on a server you are monitoring. You can then have this Action launch your script file when an event is detected. For example, enter: `cmd /c c:\winnt\fixitscript.bat`.

To ensure the command runs successfully:

- Include the full path to the executable you want to run. For example, to issue a `Ping` command, you may need to enter a command similar to the following:

  ```
  cmd /c c:\winnt\ping.exe 164.210.210.1.
  ```

- Be sure that the command you want to run does not require any user input.
- To run this Action on the managed computer, select **MC (Managed Client)** as the Location on the Action tab of the Properties dialog box.
- Check whether the computer where you want to run a command or script file accepts commands from the management server you are using. This access is controlled through the `AllowDosCmd` registry key setting. By default, the `AllowDosCmd` key is set to `*` to allow all management servers to initiate DOS commands. To restrict the management servers that are allowed to run DOS commands, you can set this key to a comma-separated list of computer names. For example, `AllowDosCmd:REG_SZ:shasta,dynamo`.
- Verify that the AppManager Client Resource Monitor (`NetIQmc`) service account, whether it be the `LocalSystem` account or a user account, has permission to execute the command you want to run on the computer where you want the Action executed.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity -- Action failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DosCommand job fails. The default is 5 (red event indicator). This parameter is not supported for AppManager version 6.x.
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	

Parameter	How to Set It
Non-interactive DOS command	Specify the command to run. Do not enter a command that requires user input. The command you enter should take care of any input and output redirection or handling required. The default is `del\temp\yunk.txt`. **Note** If the command you are entering includes quotation marks ("), enclose the quoted string in a second set of quotation marks. For example, if the DOS command is `net send "message"`, enter the following: `cmd /c net send ""message""`. You can use the following keywords in the command: • `$ShortMsg$` (short event message) • `$DetailMsg$` (detailed event message) • `$Time$` (date and time of the event) • `$JobID$` (ID of the job that raised the event) • `$MachineName$` (name of the computer where the event was raised) • `$Severity$` (severity of the event) • `$KSName$` (name of the Knowledge Script that raised the event) • `$ObjectName$` (name of the AppManager resource object where the event was raised) • `$EventID$` (event ID) For `$ShortMsg$` and `$DetailMsg$`, you can use number and wildcard options to indicate specific portions of the text string to include. For example: • `$DetailMsg$[5]` includes the fifth word of the detailed event message • `$ShortMsg$[1-5]` includes the first through fifth words of the short message event • `$DetailMsg$[*5]` includes the first through fifth words of the detailed event message • `$ShortMsg$[5*]` includes the fifth through last words of the short event message If you do not enter a word specifier, AppManager returns the entire string. **Example** To print a detail message starting from the eighth word into `c:\temp\log.txt`, type the following command: `echo $DetailMsg$[8*] > c:\temp.log.txt`
Normal/Expected exit code	Set the normal/expected exit code for the DOS command you enter. The default is 0.
Test command-line syntax?	Select **Yes** if you want to test the command-line syntax you specified for the *Non-interactive DOS command* parameter. The default is unselected.
Event severity -- Test command	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the test command runs successfully. The default is 35 (magenta event indicator).

DumpTran

Use this Action Knowledge Script with selected SQL Knowledge Scripts (such as DataSpace, DBSpace, and LogSpace) to dump the transaction log of a database when an event is raised. For example, if the DBSpace Knowledge Script detects that the database space available has fallen below the threshold, you can use this Action to automatically dump the transaction log to free up space. Syntax and permission checking is handled by SQL Server.

When configuring this action, keep in mind:

- The Action can run only on the managed computer as a Managed Client Action. Be sure to select **MC** (Managed Client) as the Location on the Action tab of the Properties dialog box.
- This script requires an account with System Administrator privileges or dbo privileges to run. If you run this Action on SQL Server 7, the Dump Transaction can be done by a dbo or db_backup operator account. For more information about the permissions required for a Dump Transaction command, see your SQL Server documentation.
- This script requires a database name supplied by the SQL Knowledge Script to perform the dump. If the Knowledge Script that raises the event is running with the *Dynamically observe databases at each interval?* parameter enabled (so that it dynamically discovers database names at run time), the Action will fail. To use this Action, disable the *Dynamically observe databases at each interval?* parameter in the DataSpace, DBSpace, or LogSpace Knowledge Script.

This Action can only operate on a database whose recovery model is either Full or Bulk-Logged.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
SQL login	Specify the database user account used to run this Knowledge Script, for example, `sa`. You can run this Knowledge Script using other user accounts that have been set up in the SQL Server of the managed client and have been given permission to run SQL Knowledge Scripts through the AppManager Security Manager.
Truncate only?	Set to **y** to truncate the transaction log, without saving the truncated information to any location. If set to n, you must specify where the transaction log should be sent in the TO statement parameter. The default is n.
TO statement	If *Truncate only?* is disabled, enter a TO statement to specify where the truncated transaction log should be sent. The default is `to diskdump`.

ExtendedSNMPTrap

Use this Knowledge Script to send an extended SNMP trap message with AppManager event information to a specified list of computers. The event information includes the event severity level.

Each computer you specify must be able to receive SNMP trap messages on UDP port 162.

If you do not specify a value for any of the parameters, this Knowledge Script uses the corresponding value found in the registry under `HKEY_LOCAL_MACHINE\Software\NetIQ\AppManager\4.0\NetIQmc\SNMPTRAP\Config`.

For example, if you do not specify an object identifier in the OID field, the Knowledge Script checks the registry for the OID key entry: `OID: REG_SZ: 1.3.6.1.4.1.1691.1`.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
List of computers to receive SNMP message	Provide the name of the computer to receive the SNMP trap message. The receiving port is port 162. To specify multiple recipients, separate computer names with commas and no spaces. For example, `Nancy01,Finance03` If this field is left blank, the local host is the recipient by default.
Community string	Provide a valid SNMP community string. Leave this parameter blank to use the SNMP community string entered in AppManager Security Manager. If no SNMP community string is entered in Security Manager, the “public” SNMP community string is used by default.
Object identifier	Enter an object identifier in OID notation (for example, 1.2.3.456.78). If no value is entered, this script uses the OID notation entered in the following registry key: `SOFTWARE\NetIQ\AppManager\4.0\NetIQmc\SNMPTRAP\Config`
Specific trap number	Enter a trap number. The trap number can be specific to your application. If no value is entered, this script uses the trap number entered in the following registry key: `SOFTWARE\NetIQ\AppManager\4.0\NetIQmc\SNMPTRAP\Config`

IISContinueSite

Use this Knowledge Script to continue a paused IIS site. This script raises an event if the script is unable to continue a paused IIS site.

This Action can run only on the managed computer as a managed client Action. Be sure to select **MC** (managed client) as the Location on the Action tab of the Properties dialog box. This Action cannot run as a management server (MS) Action.

When you use this Action with a Knowledge Script that supports dynamic observation and you enable the *Dynamic observation* parameter, you can only run the Knowledge Script on one Web site at a time. If you disable dynamic observation, you can run the Knowledge Script on all Web sites.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if attempt to continue fails?	Set to **y** to raise an event if the attempt to continue a paused IIS site fails. The default is y.
Event severity when site cannot be continued	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a paused IIS site cannot be continued. The default severity level is 7 (red event indicator).

IISPauseSite

Use this Knowledge Script to temporarily pause an IIS site. This script raises an event if the IIS site cannot be paused.

This Action can only run on the managed computer as a managed client Action. Be sure to select **MC** (managed client) as the Location on the Action tab of the Properties dialog box. This Action cannot run as a management server (MS) Action.

When you use this Action with a Knowledge Script that supports dynamic observation and you enable the *Dynamically observe Web servers at each interval* parameter, you can only run this Knowledge Script on one Web site at a time. If you disable dynamic observation, you can drop the Knowledge Script on all Web sites.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if attempt to pause fails?	Set to **y** to raise an event if the attempt to pause an IIS site fails. The default is y.
Event severity when site cannot be paused	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an IIS site cannot be paused. The default severity level is 7 (red event indicator).

IISRestartServer

Use this Knowledge Script to stop and then restart an IIS server. This script raises an event if the attempt to stop or restart a service fails or succeeds. Any services that are stopped when the job runs can also be detected and started.

When you use this Action with a Knowledge Script that supports dynamic observation and you enable the *Dynamically observe Web servers at each interval* parameter, you can only run this Knowledge Script on one Web site at a time. If you disable dynamic observation, you can run the Knowledge Script on all Web sites.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if attempt to restart fails or succeeds?	Set to **y** to raise an event if the IIS server cannot be restarted, or if the server is successfully restarted. The default is y.
Restart server?	Set to **y** to restart an IIS server. The default is y.
Start all stopped services?	Set to **y** to start all stopped services. The default is n.
Severity when restart...	Set the event severity level, from 1 to 40, to indicate the importance when the attempt to restart stopped services: **... fails**. Type a value that indicates the service is down and AppManager cannot restart it. The default is 10 (red event indicator). **... succeeds**. Type a value that indicates the service was down and AppManager successfully restarted it. The default is 20 (blue event indicator).

IISRestartSite

Use this Action Knowledge Script to shut down and restart an IIS site instance. This script raises an event if the IIS site cannot be shut down or restarted.

This Action can only run on the managed computer as a managed client action. Be sure to select **MC** (managed client) as the Location on the Action tab of the Properties dialog box. This Action cannot run as a management server (MS) Action.

When you use this Action with a Knowledge Script that supports dynamic observation and you enable the *Dynamically observe Web servers at each interval* parameter, you can only run this Knowledge Script on one Web site at a time. If you disable dynamic observation, you can run the Knowledge Script on all Web sites.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if attempt to shut down or restart fails?	Set to **y** to raise an event if the attempt to shut down or restart an IIS site instance fails. The default is y.
Restart site after shutdown?	Set to **y** to restart an IIS site after it is shut down. The default is y.
Event severity when attempt to shut down or restart IIS site fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an IIS site cannot be shut down or restarted. The default severity level is 7 (red event indicator).

MapiMail

Use this Knowledge Script to send a MAPI e-mail message with AppManager event information to a specified list of recipients.

By default, the event information includes the computer name of the managed client and the event severity. You can select additional information to include. You can also construct a custom message to send to recipients.

This script raises an event if you select the custom message format but neglect to enter any text for the custom message body. Under these circumstances, the script continues to execute and uses the standard message format.

You can attach a file to the e-mail message by entering the path to the file.

The e-mail message is sent using the Microsoft MAPI mechanism. The recipients can be one or many MAPI clients.

Note
Because Microsoft has tightened security in the most recent versions of Outlook, the NetiqMAPImail helper script only works with Outlook 2000 or Outlook 2003, SP1. That service pack is required. This action does not run on Outlook 2003 without service packs or on Outlook 2003 with SP2.

As an alternative, consider using the SMTPMail Knowledge Script.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity -- Action warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MapiMail job returns a warning. The default is 35 (magenta event indicator).
Event severity -- Action failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MapiMail job fails. The default is 5 (red event indicator).
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	
Profile name	Provide the profile name of the managed client, such as the default netiq account or an account set up specifically for the client. The profile must be an account with Mail capability.
List of recipients	Provide the e-mail address for the recipient of the message, using names in the address book. Separate multiple names with semicolons (;). For example: `Chris Lin;pat@bigcorp.com;gwest`. **Note** Be sure the names you enter are not ambiguous. If the script cannot definitively identify the recipient, mail is not sent.
Full path to mail attachment	Provide the full path to the attachment you want to send. If you are not attaching a file, leave this field blank.

Parameter	How to Set It
Message format	Select the format you want to use for the message sent by this script: • **Standard** format generates a message based upon the selections you make from the *Standard Message Options* parameters. • **Custom** format generates a message based upon the subject and message body you supply in the *Custom Message Options* parameters. The default is Standard.
Standard Message Options	
Include date/timestamp?	Select **Yes** to include the date/timestamp in the standard message. The default is unselected.
Include JobID?	Select **Yes** to include the job ID in the standard message. The default is unselected.
Include agent computer name?	Select **Yes** to include the name of the agent computer in the standard message (the computer hosting the agent that initiated the action). The default is Yes.
Include event severity?	Select **Yes** to include the severity of the event in the standard message. The default is Yes.
Include Knowledge Script name?	Select **Yes** to include the Knowledge Script name in the standard message (the Knowledge Script that initiated the Action). The default is unselected.
Include AppManager object name?	Select **Yes** to include the AppManager resource object name in the standard message (the AppManager resource object where the event was raised). The default is unselected.
Include AppManager event ID (only on MS Action)?	Select **Yes** to include the AppManager event ID in the standard message (possible only in cases when the Action is carried out by the management server). The default is unselected.
Include event detail message?	Select **Yes** to include the event detail message. The default is unselected.
Custom Message Options	
Custom message subject	Provide the text you want to use for the custom message subject line.

Parameter	How to Set It
Custom message body	Provide the text you want to include in your custom message. You can use the following keywords to indicate the information you want to include in your custom message: • `$ShortMsg$` (short event message) • `$DetailMsg$` (detailed event message) • `$Time$` (date and time of the event) • `$JobID$` (ID of the job that raised the event) • `$MachineName$` (name of the computer where the event was raised) • `$Severity$` (severity of the event) • `$KSName$` (name of the Knowledge Script that raised the event) • `$ObjectName$` (name of the AppManager resource object where the event was raised) • `$EventID$` (event ID) For `$ShortMsg$` and `$DetailMsg$` you can use number and wildcard options to indicate specific portions of the text string to include. For example: • `$DetailMsg$[5]` includes the fifth word of the detailed event message • `$ShortMsg$[1-5]` includes the first through fifth words of the short message event • `$DetailMsg$[*5]` includes the first through fifth words of the detailed event message • `$ShortMsg$[5*]` includes the fifth through last words of the short event message If you do not enter a word specifier, AppManager returns the entire string. The following are examples of the types of messages you can construct using these keywords: • Event from `$MachineName$`: The `$ShortMsg$[1-3]` has failed. The last command was `$DetailMsg$[4*]`. • A severity `$Severity$` event has occurred! Call the owner of `$MachineName$` immediately!

Messenger

Use this Knowledge Script to use the Windows Messenger service to send a message containing AppManager event information to a specified computer.

By default, the event information includes the computer name of the managed client and the event severity. You can select additional information to include.

You can also construct a custom message to send to recipients.

This script raises an event if you select the custom message format but neglect to enter any text for the custom message body. Under these circumstances, the script continues to execute and uses the standard message format.

The destination computer must be running the Windows Messenger service. To send the message to multiple computers, enter a comma-separated list of computer names.

Notes

- This Knowledge Script is not supported on Windows operating systems later than Windows Server 2003.
- If you are using this Knowledge Script to send a message from a Windows Server 2003 computer to a Windows NT 4 computer, the Messenger service must be running on both computers.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity -- Action warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Messenger job returns a warning. The default is 35 (magenta event indicator).
Event severity -- Action failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Messenger job fails. The default is 5 (red event indicator).
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	
List of computers to receive message	Provide a computer name or click the **Browse [...]** button to select the recipient of the Messenger service message. To send a message to multiple recipients, enter a comma-separated list of computer names. For example: `QELAB,PORT1,Chris`. Each specified computer must be running the Messenger service.
Message format	Select whether you want to use the standard message format or create a custom message. The default is Standard. Use the Standard message format if you want the message text to be generated by the Knowledge Script. Use the Custom message format if you want to create your own message.
Standard message options	

Parameter	How to Set It
Include date/timestamp?	Select **Yes** to include the date and time of the event. The default is unselected.
Include JobID?	Select **Yes** to include the ID of the Knowledge Script job that raised the event. The default is unselected.
Include agent computer name?	Select **Yes** to include the name of the computer on which the event was raised. The default is Yes.
Include event severity?	Select **Yes** to include the event severity. The default is Yes.
Include Knowledge Script name?	Select **Yes** to include the name of the Knowledge Script that raised the event. The default is unselected.
Include AppManager object name?	Select **Yes** to include the name of the AppManager object where the event was raised. The default is unselected.
Include AppManager Event ID (only on MS action)?	Select **Yes** to include the event ID number when the Action is initiated by the AppManager management server. The default is unselected.
Include event detail message?	Select **Yes** to include the event detail message. The default is unselected.

Custom message options

Parameter	How to Set It
Custom text (can include substitutions)	Provide the text you want to include in your custom message. You can use the following keywords to indicate the information you want to include in your custom message: • `$ShortMsg$` (short event message) • `$DetailMsg$` (detailed event message) • `$Time$` (date and time of the event) • `$JobID$` (ID of the job that raised the event) • `$MachineName$` (name of the computer where the event was raised) • `$Severity$` (severity of the event) • `$KSName$` (name of the Knowledge Script that raised the event) • `$ObjectName$` (name of the AppManager resource object where the event was raised) • `$EventID$` (event ID) For `$ShortMsg$` and `$DetailMsg$` you can use number and wildcard options to indicate specific portions of the text string to include. For example: • `$DetailMsg$[5]` includes the fifth word of the detailed event message • `$ShortMsg$[1-5]` includes the first through fifth words of the short message event • `$DetailMsg$[*5]` includes the first through fifth words of the detailed event message • `$ShortMsg$[5*]` includes the fifth through last words of the short event message If you do not enter a word specifier, AppManager returns the entire string. The following are examples of the types of messages you can construct using these keywords: • Event from `$MachineName$`: The `$ShortMsg$[1-3]` has failed. The last command was `$DetailMsg$[4*]`. • A severity `$Severity$` event has occurred! Call the owner of `$MachineName$` immediately!
Retry count	Set the number of time this script attempts to send the message. The default is 5.

NetAppFilerDoSnapMirror

Use this Knowledge Script to open a Telnet session on the specified Network Appliance filer and issue a `snapmirror` command. You should customize the command for your environment.

To issue a `snapmirror` command with no customization, use the NetAppFiler_DoSnapMirror Knowledge Script.

This Knowledge Script raises an event each time the Action runs. The event message displays the results of the `snapmirror` command.

Tip
A Network Appliance filer can have only one open Telnet session at a time. If a Telnet session is open when this Knowledge Script runs, the Knowledge Script job cannot issue the command and creates an event with a "Too Many Users" message. If this happens, you must wait for the next job iteration to detect the event condition and run this Action.

Setting Parameter Values

Set the following parameter as needed:

Parameter	How to Set It
Command to execute	Enter a Network Appliance filer non-interactive maintenance command. Enter a command as you would from a Telnet session. You do not need to enclose the command in quotation marks. The default is `snapmirror update`.

NetAppFilerIssueCommand

Use this Knowledge Script to open a Telnet session on the specified Network Appliance filer and issue a non-interactive maintenance command.

To simply issue a maintenance command, use the NetAppFiler_IssueCommand Knowledge Script.

This Knowledge Script does not support multi-line commands or interactive behavior.

This Knowledge Script raises an event each time the job runs. The event message displays the results of the maintenance command.

Tip
A Network Appliance filer can have only one open Telnet session at a time. If a Telnet session is open when this Knowledge Script runs, the Knowledge Script job cannot issue the command and creates an event with a "Too Many Users" message. If this happens, you must wait for the next job iteration to detect the event condition and run this Action.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Command to execute	Specify the Network Appliance filer non-interactive maintenance command you want to execute. Enter a command as you would from a Telnet session. You do not need to enclose the command in quotation marks. The default, ?, returns a list of all Network Appliance filer maintenance commands.

NetAppFilerReboot

Use this Knowledge Script to Telnet into a specified Network Appliance filer and issue a `reboot` command.

To only issue a `reboot` command, use the NetAppFiler_Reboot Knowledge Script.

This Knowledge Script raises an event each time the job runs. The event message displays the results of the `reboot` command.

Tip
A Network Appliance filer can have only one open Telnet session at a time. If a Telnet session is open when this Knowledge Script runs, the Knowledge Script job cannot issue the command and creates an event with a "Too Many Users" message. If this happens, you must wait for the next job iteration to detect the event condition and run this Action.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Reboot filer?	Set to **y** to reboot the Network Appliance filer. To avoid an accidental reboot, the default is n.

NotesMail

Use this Knowledge Script to send a mail message containing AppManager event information to one or more Lotus Domino/Notes e-mail users. To use this script, you must have a Domino Notes server, and the Notes server must be on the computer initiating the Action, either on the management server or on the managed client.

By default, the event information includes the computer name of the managed client and the event severity. You can select additional information to include.

You can also construct a custom message to send.

This script raises an event if you select the custom message format but neglect to enter any text for the custom message body. Under these circumstances, the script continues to execute and uses the standard message format.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity -- Action warning	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the NotesMail job returns a warning. The default is 35 (magenta event indicator).
Event severity -- Action failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the NotesMail job fails. The default is 5 (red event indicator).
Severity Configuration	
Minimum event severity for Action	Set the minimum event severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum event severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	
List of recipients (comma-separated; form is "`user/company`")	Provide a list of recipients for the message, separated by commas (,) with no spaces, using the Notes username format (for example, `user/company`).
Sender name	Provide the mail sender name. It is displayed in the **From** field of the mail message that has the AppManager event information. The default is NetIQ AppManager.
Message format	Select the format you want to use for the message sent by this script: • **Standard** format generates a message based upon the selections you make from the *Standard message options* parameters. • **Custom** format generates a message based upon the subject and message body you supply in the *Custom message options* parameters. The default is Standard.
Standard message options	
Include date/timestamp?	Select **Yes** to include the date/timestamp in the standard message. The default is unselected.

Parameter	How to Set It
Include JobID?	Select **Yes** to include the job ID in the standard message. The default is unselected.
Include agent computer name?	Select **Yes** to include the name of the agent computer in the standard message (the computer hosting the agent that initiated the Action). The default is Yes.
Include event severity?	Select **Yes** to include the severity of the event in the standard message. The default is Yes.
Include Knowledge Script name?	Select **Yes** to include the Knowledge Script name in the standard message (the Knowledge Script that initiated the Action). The default is unselected.
Include AppManager object name?	Select **Yes** to include the AppManager resource object name in the standard message (the AppManager resource object where the event was raised). The default is unselected.
Include AppManager event ID (only on MS Action)?	Select **Yes** to include the AppManager event ID in the standard message (possible only in cases when the Action is carried out by the management server). The default is unselected.
Include event detail message?	Select **Yes** to include the event detail message. The default is unselected.
Custom message options	
Custom message subject	Provide the text you want to use for the custom message subject line.

Parameter	How to Set It
Custom message body	Provide the text you want to include in your custom message. You can use the following keywords to indicate the information you want to include in your custom message: • `$ShortMsg$` (short event message) • `$DetailMsg$` (detailed event message) • `$Time$` (date and time of the event) • `$JobID$` (ID of the job that raised the event) • `$MachineName$` (name of the computer where the event was raised) • `$Severity$` (severity of the event) • `$KSName$` (name of the Knowledge Script that raised the event) • `$ObjectName$` (name of the AppManager resource object where the event was raised) • `$EventID$` (event ID) For `$ShortMsg$` and `$DetailMsg$` you can use number and wildcard options to indicate specific portions of the text string to include. For example: • `$DetailMsg$[5]` includes the fifth word of the detailed event message • `$ShortMsg$[1-5]` includes the first through fifth words of the short message event • `$DetailMsg$[*5]` includes the first through fifth words of the detailed event message • `$ShortMsg$[5*]` includes the fifth through last words of the short event message If you do not enter a word specifier, AppManager returns the entire string. The following are examples of the types of messages you can construct using these keywords: • Event from `$MachineName$`: The `$ShortMsg$[1-3]` has failed. The last command was `$DetailMsg$[4*]`. • A severity `$Severity$` event has occurred! Call the owner of `$MachineName$` immediately!

NTEventLog

Use this Knowledge Script to write AppManager event information to the Windows event log. By default, the event is written to the Windows Application event log on the computer where the Action is initiated. You can select another event log where the event will be written, and you can select the event type: Error, Warning, or Information. You can also specify a custom event message or use the default message.

Note
This Action is performed on all physical nodes of a cluster when the NTEventLog Knowledge Script runs on a cluster server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity -- Action warning	An event is raised when you select the custom message format but neglect to enter any text for the custom message body. Under these circumstances, the script continues to execute and uses the standard message format. Set the severity level, from 1 to 40, to indicate the importance of an event in which the NTEventLog job returns a warning. The default is 35 (magenta event indicator).
Event severity -- Action failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the NTEventLog job fails. The default is 5 (red event indicator).
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	
Event log name	Select the log where the event message is written. The default is Application.
Event type	Select the type of event message. The default is Error.
Destination computer (leave blank for local computer)	Provide the name or IP address of the computer to whose log the event message is written. You can also click **Browse [...]** to select from a list of computers in the same domain as the agent computer.
Event source	Specify a name for the source of the event. The default is AppManager.
Event category	Specify a numerical identifier for the event category. Enter a number from 0 to 3276. The default is 0.
Event ID	Specify a numerical ID for the event. Enter a number from 0 to 6553. The default is 260.

Parameter	How to Set It
Message format	Select the format you want to use for the message sent by this script: • **Standard** format generates a message based upon the selections you make from the *Standard message options* parameters. • **Custom** format generates a message based upon the subject and message body you supply in the *Custom message options* parameters. The default is Standard.
Standard message options	
Include date/timestamp?	Select **Yes** to include the date/timestamp in the standard message. The default is unselected.
Include JobID?	Select **Yes** to include the job ID in the standard message. The default is unselected.
Include agent computer name?	Select **Yes** to include the name of the agent computer in the standard message (the computer hosting the agent that initiated the Action). The default is Yes.
Include event severity?	Select **Yes** to include the severity of the event in the standard message. The default is Yes.
Include Knowledge Script name?	Select **Yes** to include the Knowledge Script name in the standard message (the Knowledge Script that initiated the Action). The default is unselected.
Include AppManager object name?	Select **Yes** to include the AppManager resource object name in the standard message (the AppManager resource object where the event was raised). The default is unselected.
Include AppManager event ID (MS Action only)?	Select **Yes** to include the AppManager event ID in the standard message (possible only in cases when the Action is carried out by the management server). The default is unselected.
Include event detail message?	Select **Yes** to include the event detail message. The default is unselected.

Parameter	How to Set It
Custom message options	
Custom text (can include substitutions)	Provide the text to include in your custom message. Use the following keywords to indicate the information to include in the message: • `$ShortMsg$` (short event message) • `$DetailMsg$` (detailed event message) • `$Time$` (date and time of the event) • `$JobID$` (ID of the job that raised the event) • `$MachineName$` (name of the computer where the event was raised) • `$Severity$` (severity of the event) • `$KSName$` (name of the Knowledge Script that raised the event) • `$ObjectName$` (name of the AppManager resource object where the event was raised) • `$EventID$` (event ID) For `$ShortMsg$` and `$DetailMsg$` you can use number and wildcard options to indicate specific portions of the text string to include. For example: • `$DetailMsg$[5]` includes the fifth word of the detailed event message • `$ShortMsg$[1-5]` includes the first through fifth words of the short message event • `$DetailMsg$[*5]` includes the first through fifth words of the detailed event message • `$ShortMsg$[5*]` includes the fifth through last words of the short event message If you do not enter a word specifier, AppManager returns the entire string. The following are examples of the types of messages you can construct using these keywords: • Event from `$MachineName$`: The `$ShortMsg$[1-3]` has failed. The last command was `$DetailMsg$[4*]`. • A severity `$Severity$` event has occurred! Call the owner of `$MachineName$` immediately!

Page

Use this Knowledge Script to send a paging call with AppManager event information to one or more recipients. Paging systems and target recipients (individuals or groups) are defined in the `\winnt\netiqpage.ini` file on the AppManager repository (QDB) computer. Before using this script, review and edit the `netiqpage.ini` file to identify the groups, phone numbers, and other parameters appropriate for your specific paging system.

By default, the event information includes the name of the agent computer and the event severity. You can select additional information to include.

You can also construct a custom message to send to recipients.

This script raises an event if you select the custom message format but neglect to enter any text for the custom message body. Under these circumstances, the script continues to execute and uses the standard message format.

Example of How this Script Is Used

Because each paging system has its own command-line syntax or API requirements, you need to define some information about the paging systems you are using in the `netiqpage.ini` file before using this Knowledge Script. The `netiqpage.ini` file specifies:

- Path to the paging server interface. For example, the path to the command-line program used to send the page.
- Command-line parameters or API syntax used to construct the page. For example, a specific paging interface may require a pager number, sender ID, or start time as command line arguments.
- Target group or profile names that contain the rules for contacting groups or individuals. For example, some paging systems allow an administrator to set up templates that define contact flow to control when specific groups can be reached by pager.

The following information is defined in the `netiqpage.ini` file in two sections:

- The `[system]` section, which defines the paging system, the path to the interface, and the command line parameters to be passed in from the `[group_name]` section depending on the *Name of the group to page* you enter in the Knowledge Script.
- The `[group_name]` sections, which define the details for target groups.

The following in an example of a `netiqpage.ini` file with definitions for three paging systems and two target groups, `QA` and `Sales`:

```
;;
;; sample netiqpage.ini file
;;

[system]
;; For the command line syntax for these paging systems:
;; first %s maps to the target_name [target]
;; second %s maps additional parameters [param]
;; third %s is the message passed in from the Knowledge Script
;;
attention=c:\AttnClient\attn -t %s %s %s
telalert=c:\usr\telalert\telalertc -c %s %s -m %s
hiplink=c:\hiplink\cms\hlclp -r:%s %s -m:'%s'  ;; msg in quotes
[QA]
    pageco1=hiplink
    target1=M
    param1=
    start_time1=00/00/00 00:00:00
    stop_time1=00/00/00 23:59:59
```

```
[Sales]
    pageco1=telalert
    target1=Pager
    param1= -n 4083031937
    start_time1=00/00/00 00:00:00
    stop_time1=00/00/00 23:59:59

    pageco2=telalert
    target2=Pager
    param2= -n 4083031937
    start_time2=5/12/98 00:00:00
    stop_time2=6/30/98 00:00:00
```

The Action_Page Knowledge Script uses the information defined in this file and the Action properties entered to construct the required command line to send the page. For example, if you set the *Name of the group to page* parameter to `Sales`, AppManager sends a page to the Sales pager number (`408-303-1937`) using the `telalert` paging system.

Defining a Paging Schedule

Within the `netiqpaqe.ini` file, you can set a paging start time and end time for each person or group. This allows you to define specific periods when the individuals in a group can be paged. For example, if you have a Tech Support group with two employees who can be paged any day of the week between the hours of midnight and 8:00 a.m. and one employee who can be paged at any hour during specific dates, you might create entries similar to the following in the `netiqpaqe.ini` file:

```
[TechSupport]
    pageco1=telalert
    target1=Blake                    // Blake can be paged
    param1= -n 4083031937            // between 12:00 a.m.
    start_time1=00/00/00 24:00:00    // and 8:00 a.m.
    stop_time1=00/00/00 08:00:00     // (no start date or
                                     // end date)
    pageco2=telalert
    target2=Andy                   // Andy has the same
    param2= -n 4084551037          // schedule as Blake
    start_time2=00/00/00 24:00:00
    stop_time2=00/00/00 08:00:00

    pageco3=telalert
    target3=Alex                   // Alex can be paged any
    param3= -n 4156542200          // hour from midnight
    start_time3=7/12/98 00:00:00   // July 12, 1998 until
    stop_time3=7/30/98 10:30:00    // 10:30a.m. July 30
```

Both the `start_time` and `stop_time` parameters consist of two parts—the date and time. If you do not want to specify a start date or an end date, set the first part of the appropriate parameter to `00/00/00` (as illustrated with `Blake` and `Andy` in the example above). If you do not want to specify a start time or an end time, set the second part of the appropriate parameter to `00:00:00` (as illustrated with `Alex` in the example).

You cannot use the `start_time` and `stop_time` parameters to set up weekly scheduling. You can only define scheduling profiles or templates using parameters associated with your paging system. For example, if your paging system supports a `-s schedule_profile` command-line parameter, you can include this in the netiqpaqe.ini file as you do other parameters. For example:

```
[system]
page_app=c:\PageSysClient\sendpage -t %s -n %s %s -m %s

[WeekdayCrew]
    pageco1=page_app
    target1=scott
    param1= -n 4083031937 -s weekday_profile
                            // name of a template that
```

```
                              // allows paging Mon-Fri
start_time1=00/00/00 00:00:00
stop_time1=00/00/00 00:00:00
```

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity -- Action warning	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Page job returns a warning. The default is 35 (magenta event indicator).
Event severity -- Action failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Page job fails.
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	
Name of the group to page (in netiqpage.ini)	Provide the name of the individual or group to receive this page. Valid names are the [group_name] sections you defined in the `netiqpage.ini` file.
Send a test page to a file?	Select **Yes** to send a test page to a file. The default is unselected.
Full path to test page file	Provide the full path to the file where you want to send your test page. The default is `c:\page.log`.
Message format	Select whether you want to use the standard message or create a custom message. The default is Standard. Use the Standard message format if you want the message text to be generated by the Knowledge Script. Use the Custom message format if you want to create your own message.
Standard Message Options	
Include date/timestamp?	Select **Yes** to include the date and time of the event. The default is unselected.
Include JobID?	Select **Yes** to include the ID of the Knowledge Script job that raised the event. The default is unselected.
Include agent computer name?	Select **Yes** to include the name of the computer on which the event was raised. The default is Yes.
Include event severity?	Select **Yes** to include the event severity with the page. The default is Yes.
Include Knowledge Script name?	Select **Yes** to include the name of the Knowledge Script that raised the event. The default is unselected.
Include AppManager object name?	Select **Yes** to include the name of the AppManager object where the event was raised. The default is unselected.
Include AppManager event ID (MS Action only)?	Select **Yes** to include the event ID number when the Action is initiated by the AppManager management server. The default is unselected.
Include event detail message?	Select **Yes** to include the text of the event detail message with the page. The default is unselected.

Parameter	How to Set It
Custom Message Options	
Custom message	Provide the message, up to 255 characters, you want to send with the page. If you do not specify a message, AppManager constructs a default message including the name of the agent computer and the severity level of the event.

RebootSystem

Use this Knowledge Script to shut down and restart a computer when an event is raised. This Action can run only on the managed computer as a Managed Client Action; select *Managed Client Action* in the Knowledge Script Properties dialog box.

To run this Knowledge Script, you need to be identified as a user with administrator privileges or have been granted permission to use this Action by the AppManager administrator.

This Knowledge Script also requires a registry setting under `HKEY_LOCAL_MACHINE\Software`: `NetIQ\AppManager\4.0\NetIQmc\Security`.

By default, the `AllowReboot` registry key is set to `null` to prevent *any* management servers from rebooting clients. If you have administrative privileges, you can change the registry settings to specify individual management servers or all management servers (using the wildcard *). For example: `AllowReboot:REG_SZ:mktg02;salesNA;190.12.1.28`.

You can use the NTAdmin_RegistrySet Knowledge Script to modify the registry key with the appropriate management server computer names.

Because of an Exchange mechanism, this Knowledge Script takes some time to reboot a computer if any Exchange service is running on that computer. Before using this Action, check whether any Exchange service is running on the target computers. If any Exchange service is running:

- Consider stopping the service before starting a Knowledge Script job that uses this Action.
- Consider whether you want to use this Action Knowledge on the selected computer.
- Allow for a longer-than-normal shutdown and reboot period.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Restart computer after shutdown?	Set to **y** to automatically restart the computer after shutting down. The default is y.
Force applications with unsaved changes to be closed?	Set to **y** to force any open applications to close when shutting down. In most cases, unsaved changes will be lost. The default is y.
Message to be displayed in the shutdown dialog box	Provide the message you want displayed in the shutdown dialog box. For example, if you are forcing applications to close, you may want the shutdown message to include a warning that unsaved changes may be lost.
Number of seconds to display shutdown dialog box	Specify the number of seconds you want the shutdown dialog displayed. The default is 60 seconds.
Number of hours to wait between restarts	Specify the number of hours to wait after the last restart before attempting another reboot. This parameter allows you to prevent the Knowledge Script job from continuously shutting down and rebooting a computer. The default is 4 hours.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event when this Action Knowledge Script encounters problems in shutting down or restarting the computer. The default is 7 (red event indicator).

RestartServices

Use this Knowledge Script to stop and restart Windows services. Enter the services you want to stop and restart as a comma-separated list.

Enable the *Restart dependent services?* parameter to restart services that depend on the ones you stopped. By default, this script restarts dependent services.

Restarting dependent services can be performed only on AppManager agents version 6.0 or later.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity -- Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the RestartServices job fails. The default is 10 (red event indicator).
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	
List of services (comma-separated, no spaces)	Provide a comma-separated list of the services you want to stop and restart.
Service start/stop delay	Set the number of seconds to wait between stopping and restarting a service. The default is 30.
Restart dependent services? (6.0+)	Select **Yes** to restart services that depend on the ones you stopped. The default is Yes. For example, if you stop the `MSSQLSERVER` service, the dependent service `SQLSERVERAGENT` is also stopped. If you select **Yes**, the `MSSQLSERVER` service will be restarted, and then the `SQLSERVERAGENT` service will also be restated. If you clear this check box, any dependent services of the service you specified are stopped and not restarted. **Note** Dependent services are restarted only by AppManager agents version 6.0 and later.

RunDiscoveryCiscoCallMgr

Use this Knowledge Script to discover Cisco Unified Communication Manager resources as a result of an event raised by the CiscoCallMgr_CCM_RoleStatus Knowledge Script.

In the event of a failover from a Primary CallManager to a Backup Communication Manager, you can set the Actions tab of the CCM_RoleStatus script to run RunDiscoveryCiscoCallMgr. This Action discovers Communication Manager resources on the Backup computer and, if you have configured a monitoring policy to do so, any jobs that are running on the Primary computer will be transferred to the Backup Communication Manager.

Note
Run this script only on a management server computer. Select **MS** (management server) as the Location on the Action tab of the Properties dialog box.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
View name to use for Knowledge Script filter	Select the view by which you want to filter the list of Knowledge Scripts to choose from. For example, select Master to include all Knowledge Scripts.
Show REPORTAM Knowledge scripts?	Set to **y** to include Report scripts in the list of scripts to choose from.
Show Discovery Knowledge scripts?	Set to **y** to include Discovery scripts in the list of scripts to choose from.
Show AMAdmin Knowledge scripts?	Set to **y** to include Admin scripts in the list of scripts to choose from.
First Knowledge Script to run	From the filtered list of Knowledge Scripts, select the first script that you want to run in response to an error. The script will run using all of the default parameter values unless you select and enter information in *Parameter to pass* and *Values for parameters*.
Parameter to pass	Provide a comma-separated list of the parameters whose default values you want to change. Leave this field blank if you want to use the default values. If you select parameters in this field, you must also enter values in *Values for parameters*.
Values for parameters	Provide a comma-separated list of the values for the parameters that you want to change. For example, enter `y,y,20`. Leave this field blank if you leave *Parameters to pass* blank.
Second Knowledge Script to run	From the filtered list of Knowledge Scripts, select the second script that you want to run in response to an error. The script will run using all of the default parameter values unless you select and enter information in *Parameter to pass* and *Values for parameters*.
Parameters to pass	Provide a comma-separated list of the parameters whose default values you want to change. Leave this field blank if you want to use the default values. If you select parameters in this field, you must also enter values in *Values for parameters*.
Values for parameters	Provide a comma-separated list of the values for the parameters that you want to change. For example, enter `y,y,20`. Leave this field blank if you leave *Parameters to pass* blank.

Parameter	How to Set It
Third Knowledge Script to run	From the filtered list of Knowledge Scripts, select the third script that you want to run in response to an error. The script will run using all of the default parameter values unless you select and enter information in *Parameter to pass* and *Values for parameters*.
Parameters to pass	Provide a comma-separated list of the parameters whose default values you want to change. Leave this field blank if you want to use the default values. If you select parameters in this field, you must also enter values in *Values for parameters*.
Values for parameters	Provide a comma-separated lis of the values for the parameters that you want to change. For example, enter `y,y,20`. Leave this field blank if you leave *Parameters to pass* blank.
Use trusted connection?	Set to **y** to use the credentials of the `netiqmc` service to connect to the repository server. The default is n. If you accept the default, then you must enter a *User ID* and *Password*.
QDB Server	Specify the name of the repository server. Leave this field blank if the repository server is the local server.
QDB Database	Specify the name of the AppManager repository that manages Knowledge Script jobs. Leave this field blank to use the default repository name, `QDB`.
User ID	Specify the user ID for a non-trusted connection to the repository server. You must enter a user ID if you disabled the *Use trusted connection?* parameter.
Password	Specify the password for a non-trusted connection to the repository server. You must enter a password if you disabled the *Use trusted connection?* parameter.
Run this Knowledge Script once	Set to **y** to schedule this script to run once, overriding the default schedule of the scripts you selected. If you disable this parameter, the scripts you selected will run according to the default.
Machine to run Knowledge Script on	Specify the name of the server on which you want to run the scripts you selected. Leave this field blank if the server is the same as the server of the parent job that raised the event.

RunDiscoveryNetworkDevice

Use this Knowledge Script to discover network device resources as a result of an event raised by the NetworkDevice_Device_Uptime Knowledge Script.

In the event of a network device reboot, you can set the Device_Uptime Knowledge Script to run this Action to rediscover network device resources on the rebooted device.

Note
Run this script only on a management server computer. Select **MS** (management server) as the Location on the Action tab of the Properties dialog box.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
View name to use for KS filter	Select the view by which you want to filter the list of Knowledge Scripts to choose from. For example, select Master to include all Knowledge Scripts.
Show Report scripts?	Set to **y** to include Report scripts in the list of scripts to choose from.
Show Discovery scripts?	Set to **y** to include Discovery scripts in the list of scripts to choose from.
Show Admin scripts?	Set to **y** to include Admin scripts in the list of scripts to choose from.
First KS to run	From the filtered list of Knowledge Scripts, select the first script that you want to run in response to an error. The script will run using all of the default parameter values unless you select and enter information in the *Parameter to pass* and *Values for parameters* parameters.
Parameter to pass	Select the parameters whose default values you want to change. Leave this field blank if you want to use the default values. If you select parameters in this field, you must also enter values for the *Values for parameters* parameter.
Values for parameters	Specify the values for the parameters that you want to change. Separate the values with a comma. For example, enter `y,y,20`. Leave this field blank if you leave *Parameters to pass* blank.
Second KS to run	From the filtered list of Knowledge Scripts, select the second script that you want to run in response to an error. The script will run using all of the default parameter values unless you select and enter information for *Parameter to pass* and *Values for parameters*.
Parameters to pass	Select the parameters whose default values you want to change. Leave this field blank if you want to use the default values. If you select parameters in this field, you must then enter values for the *Values for parameters* parameter.
Values for parameters	Enter the values for the parameters that you want to change. Separate the values with a comma. For example, enter `y,y,20`. Leave this field blank if you leave the *Parameters to pass* parameter blank.
Third KS to run	From the filtered list of Knowledge Scripts, select the third script that you want to run in response to an error. The script will run using all of the default parameter values unless you select and enter information for *Parameter to pass* and *Values for parameters*.

Parameter	How to Set It
Parameters to pass	Select the parameters whose default values you want to change. Leave this field blank if you want to use the default values. If you select parameters in this field, you must also enter values for the *Values for parameters* parameter.
Values for parameters	Specify the values for the parameters that you want to change. Separate the values with a comma. For example, enter `y,y,20`. Leave this field blank if you leave *Parameters to pass* blank.
Use trusted connection?	Set to **y** to use the credentials of the `netiqmc` service to connect to the repository server. The default is n. If you accept the default, then you must enter a *User ID* and *Password*.
QDB Server	Specify the name of the repository server. Leave this field blank if the repository server is the local server.
User ID	Specify the user id for an un-trusted connection to the repository server. You must enter a user ID if you disable the *Use trusted connection?* parameter.
Password	Specify the password for an un-trusted connection to the repository server. You must enter a password if you disable the *Use trusted connection?* parameter.
Run this KS once	Set to **y** to schedule this script to run once, thereby overriding the default schedule of the scripts you have selected. If you disable this parameter, the scripts you selected will run according to the default.
Machine to run KS on	Specify the name of the server on which you want to run the scripts you selected. Leave this field blank if the server is the same as the server of the parent job that raised the event.

RunKS

Use this Knowledge Script to run other Knowledge Scripts. You can select up to three scripts. You can also specify parameter settings for the Knowledge Scripts if you do not want to use the default settings.

Note

Run this script only on a management server computer. Select **MS** (management server) as the Location on the Action tab of the Properties dialog box.

This script uses the login credentials of the `NetIQmc` service (the AppManager agent) on the management server computer.

Prerequisite

NetIQ Object Linking and Embedding (`NetIQOLE`) must be registered on the computer on which this script runs. `NetIQOLE` is an automation object that allows AppManager to be run from a command-line. For more information, see the *Administrator Guide for AppManager* at the NetIQ AppManager Documentation Web site.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity -- Action failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the RunKS job fails. The default is 5 (red event indicator).
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	
Knowledge Script Configurations	
View name to use for Knowledge Script filter	Select an Operator Console view and computer by which you can filter the list of available Knowledge Scripts. The default is Master. Selecting an Operator Console view limits the list of available Knowledge Scripts to those visible in that view. Selecting a computer further limits the list of available Knowledge Scripts to ones that can run on that computer.
Show Report scripts?	Select **Yes** to include Report scripts in the list of available Knowledge Scripts. The default is unselected.
Show Discovery scripts?	Select **Yes** to include Discovery scripts in the list of available Knowledge Scripts. The default is unselected.
Show Administrator scripts?	Select **Yes** to include all Administrator scripts (for example, AMAdmin scripts), in the list of available Knowledge Scripts. The default is unselected.
First Knowledge Script to run	Select the first Knowledge Script run by this Action script.

Parameter	How to Set It
Parameters to pass (comma-separated)	Select the parameters whose default settings you want to change (for example, a different threshold value). To change the parameters you selected, select **CLEAR SELECTION** in the Select a Parameter dialog box, then click **Finish**. Once AppManager clears the previous parameters, click **Browse [...]** again and select new parameters for which you want to change the default settings. The browser for selecting parameters lists both the parameter name as it appears in the code for the script (for example, `TH_Physical`) and the description of the parameter as it appears in the Values tab of the Knowledge Script Properties dialog box (for example, `Maximum physical memory threshold`).

Values for parameters (comma-separated)	Provide a comma-separated list of the values for the parameters you have selected in an order that mirrors the parameter selection.
	For example, if you selected the following threshold parameters from NT_MemUtil for monitoring memory use:
	`TH_Physical,TH_Virtual,TH_Paging`
	then you would enter their values as follows:
	`95,95,95`
	Note The value you enter must be in the format expected by the Knowledge Script. For example:
	• If the possible values for a parameter are numbers from 0-100, you must enter a number in that range.
	• If the possible values are `y` or `n`, then you must enter `y` or `n`.
	One exception to this is where a Knowledge Script uses a selected check box to specify a **Yes** value and a cleared check box to specify a **No** value. In this case, the underlying values are `y` or `n`, and you must enter `y` or `n`.

Second Knowledge Script to run	Select a second Knowledge Script run by this Action script.
Parameters to pass (comma-separated)	Select the parameters whose default settings you want to change (for example, a different threshold value). To change the parameters you selected, select **CLEAR SELECTION** in the Select a Parameter dialog box, then click **Finish**. Once AppManager clears the previous parameters, click **Browse [...]** again and select new parameters for which you want to change the default settings. The browser for selecting parameters lists both the parameter name as it appears in the code for the script (for example, `TH_Physical`) and the description of the parameter as it appears in the Values tab of the Knowledge Script Properties dialog box (for example, `Maximum physical memory threshold`).

Parameter	How to Set It

Values for parameters (comma-separated)	Provide a comma-separated list of the values for the parameters you have selected in an order that mirrors the parameter selection.
	For example, if you selected the following threshold parameters from NT_MemUtil for monitoring memory use:
	`TH_Physical,TH_Virtual,TH_Paging`
	then you would enter their values as follows:
	`95,95,95`
	Note The value you enter must be in the format expected by the Knowledge Script. For example:
	• If the possible values for a parameter are numbers from 0-100, you must enter a number in that range.
	• If the possible values are `y` or `n`, then you must enter `y` or `n`.
	One exception to this is where a Knowledge Script uses a selected check box to specify a **Yes** value and a cleared check box to specify a **No** value. In this case, the underlying values are `y` or `n`, and you must enter `y` or `n`.

Third KS to run	Select a third Knowledge Script run by this Action script.
Parameters to pass (comma-separated)	Select the parameters whose default settings you want to change (for example, a different threshold value). To change the parameters you selected, select **CLEAR SELECTION** in the Select A Parameter dialog box, then click **Finish**. Once AppManager clears the previous parameters, click **Browse [...]** again and select new parameters for which you want to change the default settings. The browser for selecting parameters lists both the parameter name as it appears in the code for the script (for example, `TH_Physical`) and the description of the parameter as it appears on the **Values** tab of the Knowledge Script Properties dialog box (for example, `Maximum physical memory threshold`).

Values for parameters (comma-separated)	Provide a comma-separated list of the values for the parameters you have selected in an order that mirrors the parameter selection.
	For example, if you selected the following threshold parameters from NT_MemUtil for monitoring memory use:
	`TH_Physical,TH_Virtual,TH_Paging`
	then you would enter their values as follows:
	`95,95,95`
	Note The value you enter must be in the format expected by the Knowledge Script. For example:
	• If the possible values for a parameter are numbers from 0-100, you must enter a number in that range.
	• If the possible values are `y` or `n`, then you must enter `y` or `n`.
	One exception to this is where a Knowledge Script uses a selected check box to specify a **Yes** value and a cleared check box to specify a **No** value. In this case, the underlying values are `y` or `n`, and you must enter `y` or `n`.

Run this Knowledge Script once (override default schedule)?	Select **Yes** to run the specified Knowledge Scripts only once regardless of their default schedules. The default is Yes.
Computer to run Knowledge Script (leave blank for same as parent job)	Specify the name of the computer on which the Knowledge Scripts will run, or click **Browse [...]** to select a computer in the Computer Browser dialog box. If you leave this parameter blank, the scripts will run on the same computer as the Knowledge Script that initiated the Action.

AppManager Repository Configuration

Parameter	How to Set It
Use trusted connection?	Select **Yes** to use a trusted connection when running the Knowledge Scripts. The default is Yes. If you use a trusted connection, the Knowledge Scripts run under the logon account used by the `netiqmc` service on the computer running the Knowledge Script that initiated the Action. If you do not use a trusted connection, the Knowledge Scripts run with the username and password specified in the parameters below.a
Repository server (blank for local server)	Provide the name of the SQL Server used for the AppManager repository that will manage the Knowledge Script jobs. If you leave this value blank, the local computer name is used (the local computer is the one running the Knowledge Script that initiated the Action).
Repository database (blank if name is QDB)	Provide the name of the AppManager repository that will manage the Knowledge Script jobs. If you leave this value blank, the default repository name, `QDB`, is used.
User ID (non-trusted connection)	Provide the username for the account under which the Knowledge Scripts will run (if you disabled the *Use trusted connection?* parameter).
Password (non-trusted connection)	Provide the password for the account under which the Knowledge Scripts will run (if you disabled the *Use trusted connection?* parameter).

RunPhoneInventory

Use this Knowledge Script to produce an inventory of phones on a Cisco Unified Communication Manager Publisher.

This Action launches the CiscoCallMgr_CCM_PhoneInventory Knowledge Script on the Publisher associated with the server on which you are running the CiscoCallMgr_LossOfHardwarePhones Knowledge Script. Use the Actions tab on LossOfHardwarePhones to configure RunPhoneInventory.

The inventory results file is written on the computer where the AppManager agent is running, which is the Communication Manager Publisher.

Notes

- This Action can invoke CCM_PhoneInventory only on repository computers (remote or local) that successfully communicate using Windows Authentication (a trusted connection).
- Run this script only on a management server computer. Select **MS** (management server) as the Location on the Action tab of the Properties dialog box.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Event Notification	
Severity - Action warning	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the RunPhoneInventory job returns a warning. The default is 35.
Severity - Action failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the RunPhoneInventory job fails, such as an inability to write to the file or access the database. The default is 5.
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Phone Inventory Script Configuration	
CallManager database user name	Specify the user login account that you want to use to access the Communication Manager SQL Server database. Leave this field blank to use Windows authentication.
Search Options	

Parameter	How to Set It
Select by	Choose the criteria that you want to use to create the list of phones. • Name (the default) • DirectoryNumber • Description • DevicePool • CallingSearchSpace • Partition • Subnet. If you select this option, then you must enter the subnet address in the *Selection criteria* parameter. Use the following syntax: `172.16.10.0/20`. • SubnetFilepath. If you select this option, then, in the *Selection criteria* parameter, provide the UNC or full path to a file that contains a list of subnet specifications.
Selection criteria	Specify the selection criteria for the phones to be listed. Specify the actual item or specify a pattern by using the * wildcard. For example, to monitor all the phones with device names that begin with SEP, enter `SEP*`. To specify multiple items, separate each item with a comma. For example: `SEP0009A*,SEP0009B*` The items you list must be of the same type as the *Select by* parameter. So if *Select by* is Name, then the items you list must be device names or patterns. If *Select by* is DirectoryNumber, then the items you list must be directory numbers or patterns.
Order by	Select **Name** to display the contents of the results file in order by the phone name. The default is Name. Select **DirectoryNumber** to display the contents of the results file in order by directory numbers. Select **Subnet** to display the contents of the results file in order by subnet number.
Full path to results file	Specify the full path or a UNC path to which the inventory `.csv` file should be written. The default path is `c:\Program Files\NetIQ\Temp\NetIQ_Debug\PhoneInventory.csv`
AppManager Repository Configuration	
QDB Server	Specify the name of the SQL Server used for the AppManager repository that will manage the Knowledge Script jobs. If you leave this value blank, the local computer name is used (the local computer is the one running the Knowledge Script that initiated the Action).
QDB Database	Specify the name of the AppManager repository that manages Knowledge Script jobs. If you leave this value blank, the default repository name, `QDB`, is used.

RunPowerShell

Use this Knowledge Script to run a non-interactive Microsoft Windows PowerShell `cmdlet` or PowerShell script (`.PS1` file) when an event is raised by another Knowledge Script. You can also use this script to run any command that can be run from a Windows command prompt, such as `dir c:\temp`. PowerShell accepts commands in `cmdlet`, `.PS1`, and Windows `cmd.exe` formats.

Prerequisites

- Microsoft Windows PowerShell version 1.0
- Microsoft .NET Framework 3.0
- AppManager for Windows version 7.6, at minimum

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Event Notification	
Severity - Action failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the RunPowerShell job fails. The default is 5.
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action Knowledge Script. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action Knowledge Script. The default is 40.

Parameter	How to Set It
Action	

PowerShell command to run	Provide the PowerShell `cmdlet`, PowerShell script, or Windows command you want to run. Do not provide a command that requires user input. The command should take care of any required input and output redirection or handling. You can string multiple commands together. You can use the following keywords in a command:
	• `$ShortMsg$` (short event message)
	• `$DetailMsg$` (detailed event message)
	• `$Time$` (date and time of the event)
	• `$JobID$` (ID of the job that raised the event)
	• `$MachineName$` (name of the computer where the event was raised)
	• `$Severity$` (severity of the event)
	• `$KSName$` (name of the Knowledge Script that raised the event)
	• `$ObjectName$` (name of the AppManager resource object where the event was raised)
	• `$EventID$` (event ID)
	For `$ShortMsg$` and `$DetailMsg$`, you can use number and wildcard options to indicate specific portions of a text string to include. If you do not include an option, AppManager returns the entire text string. For example:
	• `$DetailMsg$[5]` includes the fifth word of the detailed event message
	• `$ShortMsg$[1-5]` includes the first through fifth words of the short event message
	• `$DetailMsg$[*5]` includes the first through fifth words of the detailed event message
	• `$ShortMsg$[5*]` includes the fifth through last words of the short event message
	For example, the following string runs the `echo` command in PowerShell and prints the detailed event information, starting from the eigth word, into the `log.txt` file on the agent computer:
	`Echo $DetailMsg$[8*] > c:\temp\log.txt`
	Hint If the command you are entering includes quotation marks (“), enclose the quoted string within a second set of quotation marks. For example, if the command is `net send “message”`, enter the following:
	`cmd /c net send ““message““`

RunSql

Use this Knowledge Script to run SQL statements or stored procedures. You can enter the SQL statements to run, or you can supply the full path to a file from which to load SQL statements.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if SQL statement succeeds?	Set to **y** to raise an event when the SQL statement is successful. The default is y. An event is always raised if an error occurs.
SQL Server name and instance if applicable ("SQL\Instance")	You can specify a SQL Server or a SQL Server and a named instance. Use the form "`SQL\Instance`". By default, the default SQL Server instance on the computer where the Action runs is used.
SQL login	Specify the database user account that will run the SQL statements (for example, `sa`). However, it is also possible to run this Knowledge Script using other user accounts that have been set up in the SQL Server of the managed client and been given permission to run SQL Knowledge Scripts through AppManager Security Manager. **Note** In general, permission to run specific SQL commands and statements is derived from the permissions granted to the login account you are using to run this Knowledge Script. However, the dbcc command can only be run by: • `dbo` account (SQL Server 6.x or 7) • `db_backup operator` account (SQL Server 7)
Load SQL script from a file?	Set to **y** to have SQL statements read from a file. Set to **n** to enter the SQL statements in the SQL Statements field. The default is n.
Full path to SQL script file	If you are entering SQL statements from a file, provide the complete file path (for example, `F:\netiq\Sample.sql`). If the NetIQmc service is running as a system account, do not provide a path in the form of `\\machine\dir\Sample.sql`
SQL statement	Specify the T-SQL statement to be executed. The default is `sp_who2`. **Tip** Unless you are entering very simple queries, typing SQL statements into this field may be error-prone. Use the *Load SQL Script from a file* parameter to read T-SQL statements from a file. Or, if you have an AppManager Developer's license, you can check the Knowledge Script out of the repository, use the script editor to paste the desired SQL statements into the SQL Statement field, then check the modified Knowledge Script back in.
Save query results to a file?	Set to **y** to save query results to an external file. The default is n. **Note** Only the first 100 lines are written to the external file.
Full path to results file	Specify a full path to the file where you want query results saved.
Severity when SQL Statement fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SQL statement fails to run. The default is 10 (red event indicator).
Severity when SQL Statement succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SQL statement runs successfully. The default is 20 (yellow event indicator).

SendReportToPrinter

Use this Knowledge Script to send a report to the printer that acts as the default printer for the managed client computer where the Report agent is running.

When running this script, consider the following:

- Install the Report agent and the Windows Management Server on the same computer.
- On the computer where the Report agent is installed, configure the managed client to run as `user`. Ensure that this user account has a default printer configured.
- Configure the `URLMapping` registry key to change the default output path of the Report agent to `<hostname>\AMReports\report`. Use the AMAdmin_SetReportPaths Knowledge Script to change the output path.

  Note
  You can also manually configure the output path of the Report agent. At a command prompt, enter regedit. In the Registry Editor window, navigate to `NetIQ\Common\AMREPORTS`. In the right panel, right-click on **URLMapping** and select **Modify**. In the Edit String dialog box, enter `<hostname>\AMReports\report` in the **Value data** field, then click **OK**.

- To use this Action when you are configuring report properties, click the **Action** tab, click **New**, select **SendReportToPrinter**, and then change the Location to **MC**.

Configuring the Managed Client to Run As User

Before you can use SendReportToPrinter, you must create a user for the NetIQ Client Resource Monitor (`NetIQmc`, also called the managed client) service on the computer where the Report agent is installed. The log-on type for this service is probably `LocalSystem` — but you cannot enable the printer function from a `LocalSystem` logon account.

To create a user for the managed client:

7. From the Windows Control Panel of the computer you want to configure, double-click **Administrative Tools**, and then double-click **Services**.
8. Right-click **NetIQ AppManager Client Resource Monitor**, and select **Properties**.
9. Click the **Logon** tab. If `Local System account` is selected, select **This account** and enter your user ID and password in the appropriate fields.
10. Ensure the user ID and password have permission to access the AppManager repository.
11. Click **OK**. In the Services window, notice that the **Logon As** information for NetIQ AppManager Client Resource Monitor has changed from `LocalSystem` to your username.
12. In the Services window, right-click **NetIQ AppManager Client Resource Monitor** and select **Restart**. Once the service stops and restarts, it is ready to accept printer requests.

Using SendReportToPrinter to Print a PDF

You can use the SendReportToPrinter Action to print your report as a `PDF` (Portable Document Format) file. You must have PDF conversion software installed on the Report agent computer.

To print a report as a PDF:

1. Install your PDF conversion software on the Report agent computer. Refer to your PDF software documentation for details about installation and preferences.
2. On the Report agent computer, set the PDF computer as the default printer.
3. Configure your report properties.
4. On the Action tab, click **New**, select **SendReportToPrinter**, and then change **Location** to **MC**.
5. Generate your report. Look for the PDF in the default location specified by your conversion software.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if job succeeds?	Set to **y** to raise an event if the process is successful. The default is n.
Event severity when...	Set the event severity level, from 1 to 40, to indicate the importance of the event when: • **... job succeeds**. The default is 25 (blue event indicator). • **... job fails**. The default is 5 (red event indicator).

SMTPMail

Use this Knowledge Script to send an SMTP mail message with AppManager event information to a list of one or more mail recipients.

By default, the event information includes the computer name of the monitored computer and the event severity. You can include additional information by enabling the appropriate parameters.

To override the default subject and body for the e-mail message, select *Custom Message Options* parameters.

This script raises an event if you select the custom message format but neglect to enter any text for the boty of the custom message. Under these circumstances, the script continues to run using the standard message format.

Note
The event ID is not included in the default message when this Action runs on a managed client (MC) computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if SMTP server is not accessible?	Select **Yes** to raise an event if the SMTP server cannot be reached. The default is Yes.
Event severity -- SMTP server not accessible	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SMTP server cannot be reached. The default is 35 (magenta event indicator).
Event severity -- Action failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SMTPMail job fails. The default is 5 (red event indicator).
Severity Configuration	
Minimum event severity for Action	Specify the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Specify the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	
List of recipient email addresses	Provide the full e-mail address for each recipient of the message. Use semicolons (;) to separate multiple recipient addresses. For example: `chris@abc.com;pat@def.com;jw@abc.com`. **Note** The following characters are invalid in this parameter: `/ \ [ ] ; : | = , * ? < >`
Sender's email address	Provide the e-mail address of the person sending the message. **Notes** • In Microsoft Exchange Server 2007 environments, specify the sender name in SMTP format: `<name>@<domain>`. • The following characters are invalid in this parameter: `/ \ [ ] ; : | = , * ? < >`

Parameter	How to Set It
SMTP server name	Provide the host name or IP address of your SMTP server. The default is `inet01`.
SMTP port	Set the port number for your SMTP server. The default is 25.
Message format	Select the format you want to use for the message sent by this script: • **Standard** format generates a message based upon the selections you make from the *Standard message options* parameters. • **Custom** format generates a message based upon the subject and message body you supply in the *Custom message options* parameters. The default is Standard.
Ping SMTP server before sending mail message?	Select **Yes** to ping the SMTP server to verify TCP connectivity before attempting to send an e-mail to your listed recipients. The default is Yes.
Standard Message Options	
Include date/timestamp?	Select **Yes** to include the date/timestamp in the standard message. The default is unselected.
Include JobID?	Select **Yes** to include the job ID in the standard message. The default is unselected.
Include agent computer name?	Select **Yes** to include the name of the agent computer that initiated the Action in the standard message. The default is Yes.
Include event severity?	Select **Yes** to include the severity of the event in the standard message. The default is Yes.
Include Knowledge Script name?	Select **Yes** to include the name of the Knowledge Script that initiated the Action in the standard message. The default is unselected.
Include AppManager object name?	Select **Yes** to include the name of the resource object where the event was raised in the standard message. The default is unselected.
Include AppManager event ID?	Select **Yes** to include the AppManager event ID in the standard message, possible only in cases when the Action is carried out by the management server. The default is unselected.
Include event detail message?	Select **Yes** to include the event detail message. The default is unselected. **Note** In Microsoft Outlook 2003 SP2 environments, the detail message information may be unformatted and presented in one string of text, such as in the following example: `Detail Message: Memory Utilization: Top 10 Consuming Processes ========== Process Name: Rtvscan Process ID (PID): 1684 Utilization (KB): 51,528.00  Process Name: NetIQmc Process ID (PID): 3424 Utilization (KB): 23,956.00  Process Name: svchost#4 Process ID (PID): 832 Utilization (KB): 17,784.00`
Custom Message Options	

Parameter	How to Set It
Custom message subject	Provide the text you want to use for the custom message subject line.
Custom message body	Provide the text you want to include in your custom message. You can use the following keywords to indicate the information you want to include in the body of your custom message: • `$ShortMsg$` (short event message) • `$DetailMsg$` (detailed event message) • `$Time$` (date and time of the event) • `$JobID$` (ID of the job that raised the event) • `$MachineName$` (name of the computer where the event was raised) • `$Severity$` (severity of the event) • `$KSName$` (name of the Knowledge Script that raised the event) • `$ObjectName$` (name of the AppManager resource object where the event was raised) • `$EventID$` (event ID) • `$tab$` inserts four whitespace characters in the message body • `$lf$` inserts a line feed in the message body • `$crlf$` inserts a carriage-return line feed in the message body • `$cr$` inserts a carriage-return in the message body For `$ShortMsg$` and `$DetailMsg$` you can use number and wildcard options to indicate specific portions of the text string to include. For example: • `$DetailMsg$[5]` includes the fifth word of the detailed event message • `$ShortMsg$[1-5]` includes the first through fifth words of the short message event • `$DetailMsg$[*5]` includes the first through fifth words of the detailed event message • `$ShortMsg$[5*]` includes the fifth through last words of the short event message If you do not enter a keyword, AppManager returns the entire string. The following are examples of the types of messages you can construct using keywords: • Event from `$MachineName$`: The `$ShortMsg$[1-3]` has failed. The last command was `$DetailMsg$[4*]`. • A severity `$Severity$` event has occurred. Call the owner of `$MachineName$` immediately.

SMTPMailRpt

This Knowledge Script supports the report-related (ReportAM) Knowledge Scripts, which can be application-specific reports or generic reports.

Use this Knowledge Script to e-mail the first page of a report to a list of recipients.

The first page of the report contains a list of parameter values and hyperlinks to subsequent pages of the report. The hyperlinks refer to files on the computer where the report is located, so the e-mail is lightweight (approximately 6-10 KB).

For this Action to succeed, generate reports on the same computer where the Report agent is installed, and use the AMAdmin_SetReportPaths Knowledge Script to display the location of each report as a hyperlink. Run AMAdmin_SetReportPaths on the AppManager Repositories object under the Report agent.

If the Admin_SetReportPaths Knowledge Script has not been used to display report locations as hyperlinks, the hyperlinks in the e-mail message will not work.

If there is no data in the report, the e-mail message will not be sent.

The **Location** for this Action must be defined as **MC** (referring to the managed computer where the Report agent is installed), and the Report agent computer must have Internet connectivity to be able to send mail.

Note
SMTPMailRpt will not send reports to Lotus Notes client because of a limitation with Lotus Notes in displaying the PNG images. For more information, see http://www-1.ibm.com/support/docview.wss?rs=0&q1=1090737&uid=swg21090737&loc=en_US&cs=utf-8&lang=

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if SMTP server is not accessible?	Select **Yes** to raise an event when the SMTP server is not accessible. The default is Yes.
Event severity - SMTP server not accessible	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SMTP server is not accessible. The default is 35 (magenta event indicator).
Event severity -- Action failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SMTPMailRpt job fails. The default is 5 (red event indicator).
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this action. The default is 40.
Action	

Parameter	How to Set It
List of recipient email addresses	Provide the e-mail address of each individual who should receive the report, using the format <recipient>@<domain> (for example, SLAAdmin@netiq.com). Use commas (,) to separate multiple recipient addresses. **Note** The following characters are invalid in this parameter: / \ [ ] ; : | = , * ? < >
Sender's email address	Provide the e-mail address of the person sending the message. **Notes** • In Microsoft Exchange Server 2007 environments, specify the sender name in SMTP format: <name>@<domain>. • The following characters are invalid in this parameter: / \ [ ] ; : | = , * ? < >
SMTP server name	Specify the name of the SMTP mail server used to send mail from the Report agent computer.
SMTP server port	Set the port number for your SMTP server. The default is 25.
Message format	Select the format you want to use for the message sent by this script: • **Standard** format generates a message based upon the selections you make from the *Standard message options* parameters. • **Custom** format generates a message based upon the subject and message body you supply in the *Custom message options* parameters. The default is Standard.
Standard Message Options	
Include date/timestamp?	Select **Yes** to include the date/timestamp in the standard message. The default is unselected.
Include JobID?	Select **Yes** to include the job ID in the standard message. The default is unselected.
Include agent computer name?	Select **Yes** to include the name of the agent computer in the standard message (the computer hosting the agent that initiated the action). The default is Yes.
Include event severity?	Select **Yes** to include the severity of the event in the standard message. The default is Yes.
Include Knowledge Script name?	Select **Yes** to include the Knowledge Script name in the standard message (the Knowledge Script that initiated the action). The default is unselected.
Include AppManager object name?	Select **Yes** to include the AppManager resource object name in the standard message (the AppManager resource object where the event was raised). The default is unselected.
Include event detail message?	Select **Yes** to include the event detail message. The default is unselected.
Custom Message Options	

Parameter	How to Set It
Custom message subject	Provide a subject line for the e-mail message. This parameter is optional. If this parameter is not set, the report title is used for the subject line.
Custom message body	Provide the text to include in your custom message. Use the following keywords to indicate the information to include in the message: • `$ShortMsg$` (short event message) • `$DetailMsg$` (detailed event message) • `$Time$` (date and time of the event) • `$JobID$` (ID of the job that raised the event) • `$MachineName$` (name of the computer where the event was raised) • `$Severity$` (severity of the event) • `$KSName$` (name of the Knowledge Script that raised the event) • `$ObjectName$` (name of the AppManager resource object where the event was raised) • `$EventID$` (event ID) For `$ShortMsg$` and `$DetailMsg$` you can use number and wildcard options to indicate specific portions of the text string to include. For example: • `$DetailMsg$[5]` includes the fifth word of the detailed event message • `$ShortMsg$[1-5]` includes the first through fifth words of the short message event • `$DetailMsg$[*5]` includes the first through fifth words of the detailed event message • `$ShortMsg$[5*]` includes the fifth through last words of the short event message If you do not enter a word specifier, AppManager returns the entire string. The following are examples of the types of messages you can construct using these keywords: The following are examples of the types of messages you can construct using these keywords: • Event from `$MachineName$`: The `$ShortMsg$[1-3]` has failed. The last command was `$DetailMsg$[4*]`. • A severity `$Severity$` event has occurred! Call the owner of `$MachineName$` immediately!

SNMPTrap

Use this Knowledge Script to send an SNMP trap message with AppManager event information to a specified list of computers. Each computer you specify must be able to receive SNMP trap messages on UDP port 162.

If you do not specify a value for any of the parameters, this Knowledge Script uses the corresponding value found in the registry under:
`HKEY_LOCAL_MACHINE\Software\NetIQ\AppManager\4.0\NetIQmc\SNMPTRAP\Config`.

For example, if you do not specify an object identifier in the OID field, the Knowledge Script checks the registry for the OID key entry: `OID: REG_SZ: 1.3.6.1.4.1.1691.1`.

By default, the event information includes the computer name of the managed client and the event severity. You can select additional information to include by enabling the appropriate parameters.

You can also specify a custom message to forward.

This script raises an event if you select the custom message format but neglect to enter any text for the custom message body. Under these circumstances, the script continues to execute and uses the standard message format.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity -- Action warning	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMPTrap job returns a warning. The default is 35 (magenta event indicator).
Event severity -- Action failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SMPTTrap job fails. The default is 5 (red event indicator).
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	
List of computers to receive SNMP message (comma-separated)	Provide the name of the computer to receive the recipient of the SNMP trap message. The recipient computer must be able to receive SNMP traps on UDP Port 162. To specify multiple recipients, separate computer names with commas. For example, `Nancy01,Finance03`.
Community string	Provide a valid SNMP community string. Leave this parameter blank to use the SNMP community string entered in AppManager Security Manager. The default is `public`.
Object identifier	Provide an object identifier in OID notation (for example, `1.2.3.456.78`). The default is the NetIQ enterprise OID, `1.3.6.1.4.1.1691`.

Parameter	How to Set It
Specific trap number	Specify a trap number. The trap number can be specific to your application. The default is 1.
Message format	Select the format you want to use for the message sent by this script: • **Standard** format generates a message based upon the selections you make from the *Standard message options* parameters. • **Custom** format generates a message based upon the subject and message body you supply in the *Custom message options* parameters. The default is Standard.
Standard Message Options	
Include JobID?	Select **Yes** to include the job ID in the standard message. The default is unselected.
Include agent computer name?	Select **Yes** to include the name of the agent computer in the standard message (the computer hosting the agent that initiated the Action). The default is unselected.
Include event severity?	Select **Yes** to include the severity of the event in the standard message. The default is Yes.
Include Knowledge Script name?	Select **Yes** to include the Knowledge Script name in the standard message (the Knowledge Script that initiated the Action). The default is unselected.
Include AppManager object name?	Select **Yes** to include the AppManager resource object name in the standard message (the AppManager resource object where the event was raised). The default is unselected.
Include AppManager event ID (only on MS Action)?	Select **Yes** to include the AppManager event ID in the standard message (possible only in cases when the Action is carried out by the management server). The default is unselected.
Include event detail message?	Select **Yes** to include the event detail message. The default is unselected.
Custom Message Options	

Parameter	How to Set It
Custom message (can include substitutions)	Provide the text to include in your custom message. Enter the custom message text without quotes. Use the following keywords to indicate the information to include in the message: • `$ShortMsg$` (the short event message) • `$DetailMsg$` (the detailed event message) • `$Time$` (the date and time of the event) • `$JobID$` (the ID of the job that raised the event) • `$MachineName$` (the name of the computer where the event was raised) • `$Severity$` (the severity of the event) • `$KSName$` (the name of the Knowledge Script that raised the event) • `$ObjectName$` (the name of the AppManager resource object where the event was raised) • `$EventID$` (the event ID) For `$ShortMsg$` and `$DetailMsg$` you can use number and wildcard options to indicate specific portions of the text string to include. For example: • `$DetailMsg$[5]` includes the fifth word of the detailed event message • `$ShortMsg$[1-5]` includes the first through fifth words of the short message event • `$DetailMsg$[*5]` includes the first through fifth words of the detailed event message • `$ShortMsg$[5*]` includes the fifth through last words of the short event message If you do not enter a word specifier, AppManager returns the entire string. The following are examples of the types of messages you can construct using these keywords: • Event from `$MachineName$`: The `$ShortMsg$[1-3]` has failed. The last command was `$DetailMsg$[4*]`. • A severity `$Severity$` event has occurred! Call the owner of `$MachineName$` immediately!

StartServices

Use this Knowledge Script to start Windows services in response to an event.

You can specify a number of seconds to wait after initiating the `service start` command to check the status of the service and make that it was successfully started.

Note
If the service you specify has dependent services, enter the names of dependent services after the name of the primary service. For example, SQLServerAgent is a dependent service of MSSQLServer. To start MSSQLServer and its dependent service, specify `MSSQLServer,SQLServerAgent` for the *Service name(s)* parameter. In cases with multiple dependent services, specify the least dependent service first and the most dependent service last.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if service is successfully started?	Select **Yes** to raise an event when the services you specify are successfully started. The default is unselected.
Event severity -- Service started	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is successfully started. The default is 25 (blue event indicator).
Event severity -- Action Failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the StartServices job fails. The default is 10 (red event indicator). This Knowledge Script always raises an event when it is unable to start a service.
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	
Service name(s) (comma-separated, no spaces)	Provide a comma-separated list of the services you want to start. You can use the *service name* or *display name* listed in the Properties dialog box for the service. **Note** If the service you specify has dependent services, enter the names of dependent services after the primary service. For example, `SQLServerAgent` is a dependent service of `MSSQLServer`. If you want to start `MSSQLServer` and all of its dependent services, specify `MSSQLServer,SQLServerAgent`.
Service start timeout	Set the number of seconds to attempt to start the specified services before timing out. The default is 10.

StopServices

Use this Knowledge Script to stop Windows services in response to an event.

Note
If the service you specify has dependent services, you must list the dependent services before the primary service. For example, SQLServerAgent is a dependent service of MSSQLServer. To stop MSSQLServer and its dependent service, specify `SQLServerAgent,MSSQLServer` for the *Service name(s)* parameter. In cases with multiple dependent services, specify the most dependent service first and the least dependent service last.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if service is successfully stopped?	Select **Yes** to raise an event if the services you specify are successfully stopped. The default is unselected.
Event severity -- Service stopped successfully	Set the event severity level, from 1 to 40, to indicate the importance of an event in which services are successfully stopped. The default is 25 (blue event indicator). This Knowledge Script always raises an event when it is unable to stop a service.
Raise event if service is already stopped?	Select **Yes** to raise an event if the services you specify are already stopped. The default is unselected.
Event severity -- Service already stopped	Set the event severity level, from 1 to 40, to indicate the importance of an event in which specified services are already stopped. The default is 25 (blue event indicator).
Raise event if service is missing?	Select **Yes** to raise an event if the services you specify are missing. The default is unselected.
Event severity -- Service missing	Set the event severity level, from 1 to 40, to indicate the importance of an event in which specified services cannot be found. The default is 25 (blue event indicator).
Event severity -- Action failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the StopServices job fails. The default is 10 (red event indicator).
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	

Parameter	How to Set It
Service name(s) (comma-separated, no spaces)	Provide a comma-separated list of the services you want to stop. You can use the *service name* or *display name* listed in the Properties dialog box for the service. **Note** If the service you specify has dependent services, enter the dependent services before the primary service. For example, `SQLServerAgent` is a dependent service of `MSSQLServer`. If you want to stop `MSSQLServer` and all of its dependent services, specify `SQLServerAgent,MSSQLServer`.
Service stop timeout	Set the number of seconds to attempt to stop the specified services before timing out. The default is 30.

Traceroute

Use this Knowledge Script to collect exception traceroute data between a specified source and target location in response to an event in another Knowledge Script.

When you enable this script to run automatically in association with another Knowledge Script job, you must specify the source and target locations of the traceroute as parameters. The source location *must* have the ResponseTime for Networks managed object installed and discovered.

When you associate this Action with a monitoring Knowledge Script, you must set the **Location** to **MC** to run the Action on the managed client. Otherwise, this Action creates an error event and will not collect traceroute data when it is invoked.

Note
Although any managed client can be selected as the Location, the ResponseTime for Networks managed object must be installed on the managed client.

On the Actions tab, set the Action **Type** value to **Repeat Event - 1** to run a new traceroute each time an event occurs. The **Type** value is dependent on the settings for event collapsing and on the schedule of the associated Knowledge Script. If the Knowledge Script runs and generates events more often than the event collapsing interval (default is 20 minutes), the traceroute Action will not occur at every event. A new child event must be generated for the Action to be executed.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Traceroute source location	The source is where the traceroute is run from. Select a ResponseTime for Networks node. The field may not be left blank. Specify only one source.
Traceroute target location	The target is where the traceroute will be run to. Select a ResponseTime for Networks node, some other AppManager node, an IP address, or a URL. The field may not be left blank. Specify only one target. The script will validate the source and target locations are not the same, and will generate an error if they are identical.
Maximum number of hops	Set the maximum number of hops, from 1 to 30, allowed in the traceroute. The default is 30.
Event when traceroute fails?	Set to **y** to raise events if the Traceroute job fails. The default is y.
Event severity -- Traceroute failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Traceroute job fails. The default is 20.

Example of How this Script Is Used

Before you launch a Knowledge Script (other than one of the Networks-RT scripts), double-click it to see its Properties dialog box. Click the **Actions** tab. Click **New** and select **Action_Traceroute** from the list. Then click **Properties** to specify the source location and target location for the traceroute. If an event is generated by the Knowledge Script, the Action_Traceroute Knowledge Script is launched automatically. It collects traceroute data between the source and target you selected and stores the traceroute data in the AppManager repository.

The traceroute data is associated with the event that triggered the traceroute. Run the Report_TracerouteException Knowledge Script to generate a report that compares the traceroute data collected for this event with the historical traceroute data for the associated source and target locations.

TracerouteNetworks-RT

Use this Knowledge Script to collect exception traceroute data between a specified source and target location in response to an event in a separate Networks-RT Knowledge Script.

You do not have to specify source or target information when associating the Action script with the Knowledge Script. This script automatically determines the source and target locations for the traceroute, based on the event details from the Knowledge Script.

When you associate this Action with a monitoring Knowledge Script, you must set the **Location** to **MC** to run the Action on the managed client. Otherwise, this Action creates an error event and will not collect traceroute data when invoked.

Note
Although any managed client can be selected as the Location, the ResponseTime for Networks managed object must be installed on the managed client.

On the Actions tab, set the Action **Type** value to **Repeat Event - 1** to run a new traceroute each time an event occurs. The **Type** value is dependent on the settings for event collapsing and on the schedule of the associated Knowledge Script. If the Knowledge Script runs and generates events more often than the event collapsing interval (default is 20 minutes), the traceroute Action will not occur at every event. A new child event must be generated for the Action to be executed.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Maximum number of hops	Set the maximum number of hops, from 1 to 30, allowed in the traceroute. The default is 30.
Event when traceroute fails?	Set to **y** to raise an event if the TracerouteNetworks-RT job fails. The default is y.
Event severity for traceroute failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the TracerouteNetworks-RT job fails. The default is 20.

Example of How this Script Is Used

Before you launch a Networks-RT Knowledge Script, double-click it and click the **Actions** tab on the Properties dialog box. Click **New**, and select **Action_TracerouteNetworks-RT** from the list. If an event is generated by the Knowledge Script, the Action_TracerouteNetworks-RT Knowledge Script is launched automatically. It collects traceroute data between the source and target locations associated with the event, and stores the traceroute data in the AppManager database.

The traceroute data is associated with the event that triggered the traceroute. Run the Report_TracerouteException Knowledge Script to generate a report that compares the traceroute data collected for this event with the historical traceroute data for the given pair of endpoints.

UpdateEventStatus

Use this Action Knowledge Script to acknowledge or close AppManager events from one or more specified computers. If you do not specify any computer, the computer that submitted the event is used. This script raises an event if an action fails.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Severity for Action failure	Set the severity level, from 1 to 40, to indicate the importance of the event when the UpdateEventStatus job fails. The default is 5 (red event indicator).
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	
Repository Server	Provide the name of the server that hosts the AppManager repository.
Repository Database Name	Provide the name of the AppManager repository. The default is QDB.
Update event status to...	Select the update event status as closed or acknowledged. By default, the update event status is Acknowledged.
Filter Options	
Filter by computers?	Select **Yes** to filter events by computers. The default is Yes.
Filter by the computer that raised the event?	Select **Yes** to include the computer that raised the event. The default is Yes.
Filter by these computers (comma-separated list)	Select the computers or provide a comma-separated list of computer names by which you want to filter events. For example: `QELAB,PORT1,Chris`
Filter by these Knowledge Scripts (comma-separated list)	Provide a comma-separated list of Knowledge Scripts by which you want to filter events. For example, `Action_IISContinueSite,Action_Messenger,Action_Diagnose`
Filter by event severity	Specify the severity level by which you want to filter events. By default, the event severity is 1 to 40.
Filter by event message	Specify the message by which you want to filter events. The event message indicates whether or not the action was successful, and provides an explanation if the action fails.
Filter by event age	Specify the age of the event. The default is 0 minutes.
Include only events that are...	Indicate whether to include newer or older events based on the age of the event. The default is Older.

UXCommand

Use this Knowledge Script to run a non-interactive UNIX command in response to an event. For example, you can use this Knowledge Script to run a batch command for appending a log file or stopping a process.

You can include arguments in the command-line string, but you need to escape any double quote (") or special characters by typing a preceding backslash (\). Special characters for Perl-based scripts include the dollar sign ($), percentage (%), and at symbol (@). In addition, avoid using the ampersand (&), the dollar sign ($), or backquotes (`) in the command string.

Setting Parameter Values

Set the following parameter as needed:

Parameter	How to Set It
Non-interactive UNIX command	Specify the command to run. Do not enter a command that requires user input. If your command line includes double quotes or any other special characters, use a backslash to escape the characters. For example: `grep -l \“Abnormal shutdown\” applog* > /tmp/fail`. The command you enter should include all necessary arguments and handle any input and output redirection or file management required.

Example of How this Script Is Used

Use this Action is to create a script file that contains a series of commands to diagnose or correct problems on a server you are monitoring and have this Action launch your script file when an event is detected.

To run this Action on the managed UNIX computer, select **MC** (Managed Client) as the Location on the **Action** tab of the Properties dialog box. Also verify that the NetIQ UNIX agent account has permission to execute the command you want to run on the computer where you want the Action executed.

WriteMsgToFile

Use this Knowledge Script to write AppManager event information to a file.

By default, the event information includes the agent computer name and the event severity level. You can select additional information to include by enabling the appropriate parameters.

You can also construct a custom message.

An event is raised when you select the custom message format but neglect to enter any text for the custom message body. Under these circumstances, the script continues to execute and uses the standard message format.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity -- Action warning	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the WriteMsgToFile job returns a warning. The default is 35 (magenta event indicator).
Event severity -- Action failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the WriteMsgToFile job fails. The default is 5 (red event indicator).
Severity Configuration	
Minimum event severity for Action	Set the minimum severity level, from 1 to 40, for an event that triggers this Action. The default is 1.
Maximum event severity for Action	Set the maximum severity level, from 1 to 40, for an event that triggers this Action. The default is 40.
Action	
Full path to file	Provide the complete path to the file where you want to store event information or click **Browse [...]** to find the file. The default is `c:\temp\NetiQACT_Dump.txt`.
Append event information?	Select **Yes** to append event information to the specified file. If you do not select this check box, the log file is overwritten each time the Action runs. The default is Yes.
Create folder if it does not exist?	Select **Yes** to create folders specified in the file path if they do not exist. The default is Yes.
Message format	Select the format you want to use for the message sent by this script: • **Standard** format generates a message based upon the selections you make from the *Standard Message Options* parameters. • **Custom** format generates a message based upon the subject and message body you supply in the *Custom Message Options* parameters. The default is Standard.
Standard Message Options	
Include date/timestamp?	Select **Yes** to include the date/timestamp in the standard message. The default is unselected.

Parameter	How to Set It
Include JobID?	Select **Yes** to include the job ID in the standard message. The default is unselected.
Include agent computer name?	Select **Yes** to include the name of the agent computer in the standard message (the computer hosting the agent that initiated the Action). The default is Yes.
Include event severity?	Select **Yes** to include the severity of the event in the standard message. The default is Yes.
Include Knowledge Script name?	Select **Yes** to include the Knowledge Script name in the standard message (the Knowledge Script that initiated the Action). The default is unselected.
Include AppManager object name?	Select **Yes** to include the AppManager resource object name in the standard message (the AppManager resource object where the event was raised). The default is unselected.
Include AppManager event ID (only on MS Action)?	Select **Yes** to include the AppManager event ID in the standard message (possible only in cases when the Action is carried out by the management server). The default is unselected. **Note** This Knowledge Script also displays the event ID on the proxy computer.
Include event detail message?	Select **Yes** to include the event detail message. The default is unselected.

Custom Message Options

Parameter	How to Set It
Custom text (can include substitutions)	Provide the text to include in your custom message. Use the following keywords to indicate the information to include in the message: • `$ShortMsg$` (short event message) • `$DetailMsg$` (detailed event message) • `$Time$` (date and time of the event) • `$JobID$` (ID of the job that raised the event) • `$MachineName$` (name of the computer where the event was raised) • `$Severity$` (severity of the event) • `$KSName$` (name of the Knowledge Script that raised the event) • `$ObjectName$` (name of the AppManager resource object where the event was raised) • `$EventID$` (event ID) For `$ShortMsg$` and `$DetailMsg$` you can use number and wildcard options to indicate specific portions of the text string to include. For example: • `$DetailMsg$[5]` includes the fifth word of the detailed event message • `$ShortMsg$[1-5]` includes the first through fifth words of the short message event • `$DetailMsg$[*5]` includes the first through fifth words of the detailed event message • `$ShortMsg$[5*]` includes the fifth through last words of the short event message If you do not enter a word specifier, AppManager returns the entire string. The following are examples of the types of messages you can construct using these keywords: • Event from `$MachineName$`: The `$ShortMsg$[1-3]` has failed. The last command was `$DetailMsg$[4*]`. • A severity `$Severity$` event has occurred! Call the owner of `$MachineName$` immediately!

Chapter 3
AD Knowledge Scripts

To help you set up AppManager for Active Directory monitoring in accordance with NetIQ recommended best practices guidelines, five Knowledge Script Groups are provided.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
Authentications	Monitors the number of Active Directory Kerberos and NT LAN Manager (NTLM) authentications per second.
BridgeheadChange	Monitors changes to the bridgehead roles in an Active Directory.
CacheHitRate	Monitors the Active Directory cache hit rate for name resolution.
ClientSessions	Monitors the total number of Active Directory client sessions (LDAP, AB, and XDS connections).
ConnectivityObject	Verifies connectivity between the local target computer and the Active Directory object (domain, computer or user) you specify.
DatabaseSize	Monitors the Active Directory database logical disk space usage.
DCAdvertised	Checks whether the Active Directory domain controller is being advertised properly to Active Directory clients.
DCHealthMonitor	Monitors CPU and memory usage, disk space availability, and LSASS CPU and memory usage for an Active Directory domain controller.
DCInSiteConnectivity	Checks connectivity to domain controllers in the local site container.
DomainConnectivity	Monitors the connectivity between a domain controller and selected domains.
EnumerateSites	Monitors changes to sites in an Active Directory forest.
EventLog	Monitors the Windows Event Log for Active Directory entries that match your filtering criteria.
EventLog (NetLogon)	Monitors the Windows Event Log for Active Directory entries associated with the NetLogon service that match your filtering criteria.
EventLog (W32Time)	Monitors the Windows Event Log for Active Directory entries associated with the Windows Time service that match your filtering criteria.
FSMOChange	Monitors changes to Flexible Single Master Operations (FSMO) roles in an Active Directory forest.
FSMOHealth	Monitors access to the domain controllers that have been given any Flexible Single Master Operations (FSMO) role.

Knowledge Script	What It Does
FSMOPlacement	Monitors the placement of a Flexible Single Master Operations (FSMO) role in accordance with Microsoft Best Practices.
GlobalCatalogChange	Monitors changes to the list of global catalog servers defined in the forest.
GlobalCatalogHealth	Monitors access to the global catalog servers defined in the forest.
InboundReplStat	Monitors the Inbound replication rate (inbound replication requests per second) in the Active Directory, and the percentage of applied and filtered requests.
InterReplTraffic	Monitors replication traffic from the DRA (Directory Replication Agent) between Active Directory sites (intersite traffic).
IntraReplTraffic	Monitors replication traffic from the DRA (Directory Replication Agent) within an Active Directory site (intrasite traffic).
KCCConnections	Monitors the number of Knowledge Consistency Checker (KCC) connections to and from a server within a site.
KCCDisabled	Checks whether the Knowledge Consistency Checker (KCC) is enabled or disabled for a site or server. You can set this script to automatically reenable the KCC if it is disabled.
KDCRequests	Monitors the number of Active Directory requests serviced by KDC per second.
NumberOfComputers	Monitors the number of computers in a domain or organizational unit.
NumberOfDCs	Monitors changes in the number of domain controllers in a domain, site, or forest.
NumberOfGCs	Monitors changes to the number of global catalog servers in a domain, site, or forest.
NumberOfGroups	Monitors the number of groups in a domain or organizational unit.
NumberOfObjects	Monitors the number of objects in a domain or organizational unit.
NumberOfPrintQueues	Monitors the number of printer queues in a domain or organizational unit.
NumberOfUsers	Monitors the number of users in a domain or organizational unit.
NumberOfUsersLocked	Monitors the number of locked user accounts in a domain or organizational unit.
OutboundReplStat	Monitors the outbound replication rate (outbound replication requests per second) in the Active Directory, and the percentage of Applied and Filtered requests.
PropertyWatch	Monitors changes to any property of any Active Directory object.
ReadStat	Monitors the number of Active Directory read operations per second.
ReplEventLog	Scans the System log for replication errors matching your criteria.
ReplicationCheckByUSN	Monitors replication of the Active Directory using Update Sequence Numbers (USNs).
ReplicationLatency	Injects changes to Active Directory partitions and monitors replication latency.
ReplQueueLen	Monitors the queue length for unprocessed Active Directory replication synchronization requests.
ReplSysVol	Monitors SysVol folder replication.
ReportADSI_ADObjects	Summarizes the properties and related values of objects in an Active Directory domain.

Knowledge Script	What It Does
ReportADSI_GroupMembership	Summarizes all the members that belong to an Active Directory group.
ReportADSI_LocalService	Summarizes the services running on a managed computer in an Active Directory domain.
ReportADSI_LocalUser	Summarizes the local user accounts on a managed computer in an Active Directory domain.
ReportADSI_ReplicationLatency	Generates a report about Active Directory replication latency.
ReportADSI_ReplSysVol	Reports on the consistency of files in the SysVol folder of the Report Agent's corresponding domain controller and the SysVol folders of that domain controller's replication partners.
ReportADSI_ServerRoles	Summarizes the Active Directory roles for each server in the forest.
ReportADSI_UserAccountsDisabled	Generates a report listing disabled and locked accounts in an Active Directory domain.
ReportADSI_UserBadPasswordCount	Summarizes the number of failed logins due to bad passwords for accounts in an Active Directory domain.
ReportADSI_UserMemberOfMoreThanOneGroup	Summarizes the number of members that belong to more than one group in an Active Directory domain.
ReportADSI_UserPasswordExpired	Summarizes the number of accounts with expired passwords in an Active Directory domain.
ResponseTime	Monitors the connection and read response times from the target computer to a specified Active Directory domain controller.
SearchStat	Monitors the number of Active Directory search operations per second.
ServerHealth	Monitors the health of an Active Directory domain controller.
SyncRequest	Monitors Active Directory synchronization requests and the percentage of replication synchronization requests that fail.
WriteStat	Monitors the number of Active Directory write operations per second.
AD Knowledge Script Groups	
AD	Performs essential monitoring for Active Directory domain controllers using job delegation.
AD (all DCs)	Performs essential monitoring for all domain controllers.
AD (one DC per domain)	Performs essential monitoring for a single domain controller in each domain.
AD (one DC per forest)	Performs essential monitoring for a single domain controller in a forest.
AD (one DC per site)	Performs essential monitoring for a single domain controller per site.

AD Knowledge Script Job Delegation

Some Knowledge Scripts in the AD category include an optional "job delegation" feature that automatically determines where a monitoring job should run.

Job delegation lets you select the server role that should run the job. If the role-holder changes, an event is raised, and the job is delegated to the server that now holds the selected role. Forest-wide monitoring can be delegated to the Schema Master or Domain Master. Domain-wide monitoring can be delegated to the Relative ID (RID) master, the Primary Domain Controller (PDC), or the infrastructure master (IM). Site-wide monitoring can be delegated to the Inter-Site Topology Generator (ISTG).

For example, to run a Knowledge Script job on all servers in the forest that have the Domain Master role, enable job delegation and then deploy the script to all domain controllers (DCs) in the forest. The job will run only on the DC that is currently holding the Domain Master role. Anytime a DC relinquishes or assumes that role, an event informs you of the change, but the job continues to run according to its schedule, automatically delegating the monitoring tasks only to servers holding the Domain Master role. To achieve complete coverage, include all DCs in your forest when deploying the script.

The job delegation features means that you do not need to select and re-select the proper DCs for a Knowledge Script job. Instead of constantly re-deploying the script every time there is a change to a server role, you can deploy it once with a regular schedule selected. The script then automatically runs only on the DCs holding a certain server role. Nor do you have to create special server groups that let you deploy scripts to, say, a DC from every domain. Instead, you can enable job delegation and drop the script on all DCs in the forest. The job will run only on DCs holding the server role you selected — one per domain — not on every DC in the forest.

Included as part of the recommended Knowledge Script Groups (KSGs) in AppManager for Active Directory is a KSG named "AD" that uses the job delegation feature. For more information, see "AD" on page 207.

Job delegation works because the script itself performs a check to see if each server where you dropped the script is holding the role you selected for the *Delegate monitoring to the [Active Directory server role]* parameter. If a server is no longer holding that role, the script does the following:

- Raises an event notifying you of the change.
- Forces monitoring on that server to sleep for that schedule interval.

The DC that assumes the selected server role then performs the monitoring job.

The Knowledge Script job delegation feature also includes the ability to raise an event when a DC assumes the selected server role.

The following scripts offer job delegation:

- BridgeheadChange
- DCInSiteConnectivity
- DomainConnectivity
- EnumerateSites
- FSMOChange
- FSMOHealth
- FSMOPlacement
- GlobalCatalogChange
- GlobalCatalogHealth
- KCCDisabled
- NumberOfComputers
- NumberOfDCs
- NumberOfGCs
- NumberOfGroups
- NumberOfObjects
- NumberOfPrintQueues
- NumberOfUsers
- NumberOfUsersLocked

Authentications

Use this Knowledge Script to monitor the number of Kerberos and NTLM (Windows NT LAN Manager) authentications per second. This script raises an event if the number of Kerberos or NTLM authentications per second exceeds the threshold you set.

The default protocol for network authentication for computers with Windows 2000 and later is Kerberos, but because Windows 2000 also supports NTLM authentication, this script monitors both types of network authentication.

Windows requires users and workstations to receive authentication — to prove their identity — before servers allow them access to any data. Authentication monitoring of domain controllers, which do much of the work associated with authentications, should be performed for several reasons:

- A rise in authentication load indicates authentication work has failed over to this domain controller from another domain controller.
- Sustained zero Kerberos authentication levels indicate Kerberos authentication has either failed over to another domain controller, or user authentications are failing entirely.
- A jump in authentication load is very common when a virus attack is underway.
- Any non-zero NTLM authentication load indicates legacy clients are connected.
- The ratio of Kerberos to NTLM traffic is a key indicator of how much of your client base has been upgraded to Windows 2000 or later.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counters
NTDS	Kerberos Authentications
DirectoryServices	NTLM Authentications

Resource Object

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 30 minutes**.

The default interval is intended to minimize the amount of data collected. If your organization desires tight monitoring of security-related issues, you may want to decrease the interval to **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitor authentication rate	
Event Notification	
Raise event if job fails	

Description	How to Set It
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Authentications job fails. The default is 35 (magenta event indicator).
Raise event if Kerberos authentication rate exceeds threshold?	Select **Yes** to raise an event if the Kerberos authentication rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum rate of Kerberos authentications	Specify the maximum number of Kerberos authentications per second allowed during any interval before an event is raised. The default is 50 authentications per second.
Event severity when Kerberos authentication rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Kerveros authentication rate exceeds the threshold. The default is 20 (yellow event indicator).
Raise event if NTLM authentication rate exceeds threshold?	Select **Yes** to raise an event if the NTLM authentication rate exceeds the threshold you set. The default is Yes.
Event severity when NTLM authentication rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the NTLM authentication rate exceeds the threshold. The default is 20 (yellow event indicator).
Threshold -- Maximum rate of NTLM authentications	Specify the maximum number of NTLM authentications per second allowed during any interval before an event is raised. The default is 50 authentications per second.
Data Collection	
Collect data for Kerberos authentications?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of Kerberos authentication requests since the first Knowledge Script interval (the cumulative number). The default is unselected.
Collect data for NTLM authentications?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of NTLM authentication requests since the first Knowledge Script interval (the cumulative number). The default is unselected.

BridgeheadChange

Use this Knowledge Script to monitor changes to the bridgehead roles in an Active Directory forest. This script connects to the local Active Directory database of the target server and retrieves the list of bridgehead servers. In addition, this script raises an event if new bridgehead servers are added or existing bridgehead servers are dropped.

By default, Active Directory can move bridgehead servers as needed. Many large organizations manually designate which domain controllers will serve as bridgehead servers because there is significant load placed on bridgehead servers. If your organization has defined bridgeheads manually, use this script to report all bridgehead server changes. Otherwise, use this information to correlate with a condition of high CPU utilization. If they match, the bridgehead function is the cause of the high CPU load.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the BridgeheadChange job fails. The default is 35 (magenta event indicator).
Monitor bridgehead server changes	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role (Domain Master or Schema Master) that you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate forest-wide monitoring to the	Select the server role to which the job should be delegated: **Domain Master** or **Schema Master**. By default, the job is delegated to the Domain Master.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to enable events if the DC assumes the server role you selected for the *Delegate forest-wide monitoring to the...* parameter. The event message indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to enable events if the DC gives up the server role you selected for the *Delegate forest-wide monitoring to the...* parameter. The event message indicates that the monitored computer has relinquished the selected role. The default is Yes.

Description	How to Set It
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Event Notification	
Raise event if changes to bridgehead servers are detected?	Select **Yes** to raise an event if changes to the bridgehead servers are detected. The default is Yes.
Event severity when changes detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which changes to the bridgehead servers are detected. The default is 25 (blue event indicator).
Data Collection	
Collect data for changes to bridgehead servers?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of bridgehead servers for the interval. The default is unselected.

CacheHitRate

Use this Knowledge Script to monitor the cache hit rate for the LSASS process. The cache hit rate is the percentage of time that a requested name is found in the Active Directory cache. This script raises an event if the cache hit rate falls below the threshold you set, which may indicate that you need to re-organize the Active Directory.

LSASS is the process responsible for core Active Directory functions performed using LDAP (Lightweight Directory Access Protocol). Ideally, all LDAP requests can be fulfilled out of RAM. However, when the cache hit rate falls below 95%, Active Directory performance falls off quickly. By 93%, Active Directory is typically unusable.

Tip
If the cache hit rate is low, consider adding physical RAM to the computer, or adding the /3GB switch to the boot.ini file.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counter
NTDS DirectoryServces	DS Name Cache hit rate

Resource Object

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

The default settings for the **Advanced** tab on the Properties dialog box are overridden for this script. Specifically, the *Collapse duplicates* option is disabled, and the *Raise event if event condition occurs* option is set to 3 times within 3 job iterations.

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CacheHitRate job fails. The default is 35 (magenta event indicator).
Monitor cache hit rate	
Event Notification	
Raise event if cache hit rate falls below threshold?	Select **Yes** to raise an event if the cache hit rate falls below the threshold you set. The default is Yes.

Description	How to Set It
Threshold -- Minimum cache hit rate	Specify the minimum percentage of time that requested data should be found in the cache before an event is raised. The default is 93%.
Event severity when cache hit rate falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the cache hit rate falls below the threshold. The default is 20 (yellow event indicator).
Data Collection	
Collect data for cache hit rate?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the name cache hit rate for the interval. By default, data is not collected.

ClientSessions

Use this Knowledge Script to monitor the number of Active Directory client sessions. Typically, there are three types of clients that need to access the Active Directory:

- LDAP clients
- Address book clients (AB clients)
- External and foreign directory clients (XDS clients)

The Active Directory system administrator configures a maximum number of threads to service each of these clients. With this script, you can set a threshold for maximum number of active clients sessions across all client session types. This script raises an event if the total number of client sessions exceeds the threshold you set.

A sudden surge in the number of clients may indicate that either another domain controller has gone offline, or that a change in the Active Directory subnet definitions has defined this DC as "closest."

If a surge is due to a change in Active Directory subnet definitions, then the DC being monitored may indeed be the closest server, in which case you should close the event. If this is not the intended closest DC, re-check your definitions to see why the expected DC is not in the correct site.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counters
NTDS	LDAP Client Sessions
DirectoryServices	AB Client Sessions
	XDS Client Sessions (Windows 2000 Server only)

The total number of client sessions is calculated using the following formula:

```
(Number of AB client sessions + Number of LDAP client sessions + Number of XDS client
sessions [Windows 2000 server only])
```

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ClientSessions job fails. The default is 35 (magenta event indicator).
Monitor number of client sessions	

Description	How to Set It
Event Notification	
Raise event if number of client sessions exceeds threshold?	Select **Yes** to raise an event if the number of client sessions exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of client sessions	Specify the maximum number of active client sessions allowed during an interval before an event is raised. The default is -1 sessions. You must change the default setting to run this script. You should first collect data to establish a baseline, then specify a threshold appropriate to your environment.
Event severity when client sessions exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of client sessions exceeds the threshold you set. The default is 20 (yellow event indicator).
Data Collection	
Collect data for number of client sessions?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of client sessions of each type for the interval. The default is unselected.

Example of Using this Knowledge Script

This script monitors all three types of client sessions and raises an event if the total number of client sessions exceeds the threshold. Although the event is based on the total number of client sessions, the script collects data for each type of client session separately. Because you can collect data on the number of sessions for each client type, one way you can use this script is to analyze your client session usage and compare the usage patterns to your Active Directory configuration.

For example, assume you have configured the ATQ (Asynchronous Thread Queue) for LDAP to use a maximum of 100 threads. If you enable data collection, you can keep track of the number of LDAP client sessions detected at each interval. If you see a steady increase, you may want to check for stale or hung LDAP client sessions, which are sessions that have not timed out properly. If hung client sessions are not the cause of the problem and the computer is frequently near the maximum thread limit, you may need to increase the number of ATQ threads for servicing the LDAP clients.

You can also use the *Number of consecutive occurrences before raising an event* option, on the **Advanced** tab of the Properties dialog box, to determine whether client session activity is an ongoing problem or simply an unusual spike in activity.

ConnectivityObject

Use this Knowledge Script to verify connectivity between the target computer and the Active Directory objects (domains, computers, or users) you specify. This script raises an event if the computer cannot connect to the Active Directory object you specified.

Resource Objects

Any Windows computer

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ConnectivityObject job fails. The default is 35 (magenta event indicator).
Monitor connectivity to an Active Directory object	
Active Directory object type	Select the Active Directory object to which you want to check connectivity: **domain**, **computer**, or **user**. The default is domain.
Object name (for user, type Domain/username)	Specify the name of the object to which you are checking connectivity. For example, if you specified the "domain" object, type the name of the domain to which you want to check connectivity. If you specified the "user" object, type the full user account name, including the domain. For example: `NC/wolfpack` The default entry is `rootDSE`.
Event Notification	
Raise event if connection fails?	Select **Yes** to raise an event if connection to the object fails. The default is Yes.
Event severity when connection fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which connection to the object fails. The default is 10 (red event indicator).
Data Collection	
Collect data for connection status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • 100 -- the connection was successful, or • 0 -- the object is not accessible. The default is unselected.

DatabaseSize

Use this Knowledge Script to monitor logical disk space used by the Active Directory database file on a domain controller. This script monitors the percentage of disk space used and the database size (in MB). In addition, this script raises an event if the percentage of logical disk space used exceeds the threshold you set.

Lack of disk space prevents password changes and user adds and deletes, and causes many other problems. Correcting an out-of-disk space situation may involve adding additional hardware and/or moving the database to a different drive, both of which involve extended outages.

Warning
If multiple domain controllers suddenly alert with the database growth problems, a replication storm may be occurring. Multiple DCs all running out of disk space concurrently can disable the entire company and be extremely costly and time-consuming to fix.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DatabaseSize job fails. The default is 35 (magenta event indicator).
Monitor database size	
Event Notification	
Raise event if disk space usage exceeds threshold?	Select **Yes** to raise an event if disk space usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum percentage of disk space used	Specify the maximum percentage of logical disk space that can be used by the Active Directory database file before an event is raised. The default is 80%.
Event severity when disk space usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which disk space usage exceeds the threshold. The default is 5 (red event indicator).
Data Collection	

Description	How to Set It
Collect data for database disk space usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of disk space used by the database. The default is unselected.
Collect data for database size?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the size (in MB) of the database. The default is unselected. **Tip** It is a good idea to enable data collection if you are planning to migrate data to your Active Directory domain or to add large numbers of objects, such as users or computers.

DCAdvertised

Use this Knowledge Script to check whether an Active Directory domain controller (DC) is being advertised to Active Directory clients. This script performs a DC Locator lookup to verify that the DC is being advertised in DNS properly. In addition, this script raises an event if the DC is not being advertised.

This script monitors the `netlogon` process to ensure it is advertising the correct SRV (or service) records in DNS. These records are required by Active Directory so that clients can "find" Active Directory domain controllers. If a domain controller is not properly advertised, the domain controller will be under utilized because it cannot be found.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DCAdvertised job fails. The default is 35 (magenta event indicator).
Monitor directory service availability	
Event Notification	
Raise event if directory service is unavailable?	Select **Yes** to raise an event if the directory service is unavailable. The default is Yes.
Event severity when directory service is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a directory service is unavailable. The default is 10 (red event indicator).
Data Collection	
Collect data for directory service availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • 100 -- the domain controller is advertising, or • 0 -- the domain controller is not advertising. The default is unselected.

DCHealthMonitor

Use this Knowledge Script to monitor CPU and memory usage, and disk space availability for an Active Directory domain controller. You can also use this script to monitor the CPU and memory usage for the `LSASS` process. This script raises an event if a monitored value exceeds the threshold you set.

LSASS, the Windows Local Security Authority Server process, handles Windows security mechanisms. It verifies the validity of user logons to your computer or server. Technically, the software generates the process that is responsible for authenticating users for the `Winlogon` service.

Tip
If you use this script, you should not need to do additional base OS monitoring for CPU, memory, or disk.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

The default settings for the **Advanced** tab on the Properties dialog box are overridden for this script. Specifically, the *Collapse duplicates* option is disabled, and the *Raise event if event condition occurs* option is set to 3 times within 3 job iterations.

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DCHealthMonitor job fails. The default is 35 (magenta event indicator).
Monitor CPU, memory, and disk utilization?	
Event Notification	
Raise event if CPU utilization exceeds threshold?	Select **Yes** to raise an event if CPU usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum CPU utilization	Specify the maximum percentage of CPU resources that can be used by the Active Directory domain controller before an event is raised. The default is 90%.
Event severity when CPU utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 5 (red event indicator).
Raise event if memory utilization exceeds threshold?	Select **Yes** to raise an event if memory usage exceeds the threshold you set. The default is Yes.

Description	How to Set It
Threshold -- Maximum memory utilization	Specify the maximum percentage of memory resources that can be used by the Active Directory domain controller before an event is raised. The default is 90%
Event severity when memory utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. The default is 5 (red event indicator).
Raise event if disk utilization exceeds threshold?	Select **Yes** to raise an event is disk usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum disk utilization	Specify the maximum percentage of disk space that can be used by the Active Directory domain controller before an event is raised. The default is 90%.
Event severity when disk utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which disk usage exceeds the threshold. The default is 5 (red event indicator).
Data Collection	
Collect data for system CPU utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the CPU usage of the server as a percentage of total CPU time. The default is unselected. **Tip** Enable this parameter for domain controller load trend analysis.
Collect data for system memory utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the memory usage of the server (as a percentage of total system memory). The default is unselected. **Tip** Enable this parameter for domain controller load trend analysis.
Collect data for disk utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the disk usage of the server (as a percentage of total disk space). The default is unselected. **Tip** Enable this parameter for domain controller load trend analysis.
Monitor memory and CPU for LSASS?	Select **Yes** to monitor CPU and memory usage of the LSASS process. The default is Yes.
Event Notification	
Raise event if LSASS CPU utilization exceeds threshold?	Select **Yes** to raise an event if LSASS CPU usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum LSASS CPU usage	Specify the maximum percentage of CPU resources that can be used by LSASS before an event is raised. The default is 90%.
Event severity when LSASS CPU utilization exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which LSASS CPU usage exceeds the threshold. The default is 5 (red event indicator).
Raise event if LSASS memory utilization exceeds threshold?	Select **Yes** to raise an event if LSASS memory usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum LSASS memory usage	Specify the maximum amount of memory (in KB) that can be used by LSASS before an event is raised. The default is 1700000 KB (1.7 GB). **Note** Set this parameter to 2700000 (2.7 GB) if the "/3GB" option is enabled in the `boot.ini` file.
Event severity when LSASS memory utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which LSASS memory usage exceeds the threshold. The default is 5 (red event indicator).
Data Collection	

Description	How to Set It
Collect data for LSASS CPU utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the CPU usage of the LSASS process as a percentage of total CPU time. The default is unselected. **Tip** Enable this parameter for domain controller load trend analysis.
Collect data for LSASS memory utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the memory usage of the LSASS process as a percentage of total LSASS memory. The default is unselected. **Tip** Enable this parameter for domain controller load trend analysis.

DCInSiteConnectivity

Use this Knowledge Script to check the connectivity to domain controllers in the local site. This script raises an event if connectivity to any Active Directory domain controller in the site fails.

Resource Objects

Active Directory site container on a domain controller

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DCInSiteConnectivity job fails. The default is 35 (magenta event indicator).
Monitor connectivity to DCs in the same site	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the Inter-Site Topology Generator (ISTG) server role. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate site-wide monitoring to the	Indicates the server role to which the job should be delegated, the ISTG.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** check box to raise an event if the domain controller (DC) assumes the ISTG server role. The event indicates that the monitored computer has assumed that role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the ISTG server role. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise an event if the DC gives up the ISTG server role. The event indicates that the monitored computer has relinquished that role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the ISTG server role. The default is 30 (blue event indicator).
Event Notification	
Raise event when connectivity to domain controller fails?	Select **Yes** to raise an event if connectivity to the DC fails. The default is Yes.
Event severity when domain controller down	Set the severity level, from 1 to 40, to indicate the importance of an event in which connectivity to the DC fails. The default is 5 (red event indicator).

Description	How to Set It
Data Collection	
Collect data for site connectivity percentage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the connectivity percentage for the site. For example, if 9 of the 10 domain controllers in the site are accessible, connectivity is 90%. The default is unselected.

DomainConnectivity

Use this Knowledge Script to monitor the connectivity between a domain controller and selected domains included in the scope of the target: domains included in the drop target or selected on the **Objects** tab. This script raises an event if the connection to any trusted domain fails.

Trust relationships are fragile, and problems with them hard to diagnose. Broken trusts prevent users from logging in or accessing cross-domain resources.

The most common reason for broken trust relationships are:

- No domain controllers are available for a remote domain.
- Trust password is not synchronized properly.

Resource Objects

Active Directory trusted domain

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DomainConnectivity job fails. The default is 35 (magenta event indicator).
Monitor connectivity to selected domains	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise an event if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise an event if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.

Description	How to Set It
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Event Notification	
Raise event when domain connectivity fails?	Select **Yes** to raise an event if connectivity to a domain fails. The default is Yes.
Event severity when domain connectivity fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which connectivity to a domain fails. The default is 10 (red event indicator).
Data Collection	
Collect data for connection status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • 100 -- the connection to a trusted domain was successful, or • 0 -- the connection failed. The default is unselected.

EnumerateSites

Use this Knowledge Script to monitor changes to sites in an Active Directory forest. This script raises an event if any changes since the last job iteration are detected.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the EnumerateSites job fails. The default is 35 (magenta event indicator).
Monitor the number of sites in forest	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role (Domain Master or Schema Master) that you selected for the *Delegate forest-wide monitoring to the...* parameter (see below). The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate forest-wide monitoring to the	Select the server role to which the job should be delegated: **Domain Master** or **Schema Master**. The default is Domain Master.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise an event if the DC assumes the server role you selected for the *Delegate forest-wide monitoring to the...* parameter. The event message indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise an event if the DC gives up the server role you selected for the *Delegate forest-wide monitoring to the...* parameter. The event message indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Event Notification	
Raise event when changes to sites occur?	Select **Yes** to raise an event if changes occur to sites in the forest. The default is Yes.

Description	How to Set It
Event severity when number of sites changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which changes occur to sites in the forest. The default is 25 (blue event indicator).
Data Collection	
Collect data for number of sites in forest?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of sites. The default is unselected.

EventLog

Use this Knowledge Script to monitor the Directory Service Log for Active Directory error and entries. You can configure this script to scan the log only for entries that match a set of filtering criteria.

This script does not fully rescan the event log each time it runs. All event-log entries that match the filtering criteria are returned in the event or data point detail message.

You can restrict the types of log entries that generate an event by using the *Filtering* parameters:

- Use the *Event Type* parameters to search only certain types of events, such as Warning events.
- Use the *Other* parameters to search only for specific information, such as events associated with a specific user or computer name.

Notes

- Only the most recent batch of events can be viewed in the data point detail message. For example, assume you set the script to scan all previous entries in the event log and list ten matching entries in each event detail message. When the script runs, 30 entries are found that match your filtering criteria. In this case, the script would create three child events for the interval. Each child event would have ten entries: the oldest matching entries in one child event batch, the second oldest in a second batch, and the most recent in a third batch. If this same job is collecting data and you view the detail message for the interval, only the entries from the third child event (Batch 3) are displayed.
- If you are notified of an error with **Event ID: 1311**, it is extremely important to follow the instructions provided in the error message to resolve this problem. The details that identify this event are as follows:
  - Event Type: `Error`
  - Event Source: `NTDS KCC`
  - Category: `Knowledge Consistency Checker`
  - Event ID: `1311`

Resource Object

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the EventLog job fails. The default is 35 (magenta event indicator).
Monitor Directory Service log events	

Description	How to Set It
Start with events in past N hours	Set this parameter to control checking for the first job iteration. After the first iteration, checking of the log is incremental: • **-1**--all the existing log entries • **n**--entries from the past *n* hours (8 for the past 8 hours, 50 for the past 50 hours, etc.) • **0**--no previous entries (only search from the present moment forward) The default is 0.
Filtering	
Event Types	
Error	Select **Yes** to monitor Error entries. The default is Yes.
Warning	Select **Yes** to monitor Warning entries. The default is unselected.
Information	Select **Yes** to monitor Information entries. The default is unselected.
Success Audit	Select **Yes** to monitor Success Audit entries. The default is unselected.
Failure Audit	Select **Yes** to monitor Failure Audit entries. The default is unselected.
Other	
Filter -- Source	To monitor events generated by a particular source, enter an appropriate search string. This script looks for matching entries in the Event Log's **Source** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Category	To monitor events in a particular category, such as Server or Logon, enter an appropriate search string. This script looks for matching entries in the Event Log's **Category** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Event ID	To monitor particular event IDs, enter an appropriate search string or ID range, for example, 100-2000. This script looks for matching entries in the Event Log's **Event** field. Multiple IDs and ranges can be entered, separated by commas and no spaces. For example: `1,2,10-15,202`. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- User	To monitor events associated with a particular user, enter an appropriate search string, for example, `<domain name>\<user name>`. This script looks for matching entries in the Event Log's **User** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Computer	To monitor events generated by a particular computer, enter an appropriate search string. This script looks for matching entries in the Event Log's **Computer** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.

Description	How to Set It
Filter -- Description	To monitor events with a particular detail description or containing keywords in the description, enter an appropriate search string. This script looks for matching entries in the Event Log's **Description** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Event Notification	
Raise event if new log entries found?	Select **Yes** to raise an event if new log entries are found. The default is Yes.
Maximum number of entries per event message	Specify the maximum number of entries to be recorded into each event's detail message. If this script finds more entries from the log than can be put into one event message, it will return multiple events to report all the outstanding entries in the log. The default is 1 entry.
Event severity when new event log entries found	Set the event severity level, from 1 to 40, to indicate the importance of annt in which event log entries are found. The default is 10 (red event indicator).
Data Collection	
Collect data for number of matching entries?	Select **Yes** to collect data for charts and reports. If enabled, rdata collection eturns the number of Event Log entries that match your filtering criteria. Additional information is supplied in the data detail message. The default is unselected.

EventLog (NetLogon)

Use this Knowledge Script to monitor the Windows Event Log for Active Directory entries associated with the NetLogon service. You can configure this script to scan the log only for entries that match a set of filtering criteria.

This script does not fully rescan the event log each time it runs. All event-log entries that match the filtering criteria are returned in the event or data point detail message.

You can restrict the types of log entries that generate an event by using the *Filtering* parameters:

- Use the *Event Type* parameters to search only certain types of events, such as Warning events.
- Use the *Other* parameters to search only for specific information, such as events associated with a specific user or computer name.

Note
Only the most recent batch of events can be viewed in the data point detail message. For example, assume you set this script to scan all previous entries in the event log and list ten matching entries in each event detail message. When the script runs, 30 entries are found that match your filtering criteria. In this case, the script would create three child events for the interval. Each child event would have ten entries: the oldest matching entries in one child event batch, the second oldest in a second batch, and the most recent in a third batch. If this same job is collecting data and you view the detail message for the interval, only the entries from the third child event (Batch 3) are displayed.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the EventLog (NetLogon) job fails. The default is 35 (magenta event indicator).
Monitor Windows System log for NetLogon events	
Start with events in past	Set this parameter to control checking for the first job iteration. After the first iteration, checking of the log is incremental: • **-1**--all the existing log entries • **n**--entries from the past *n* hours (8 for the past 8 hours, 50 for the past 50 hours, etc.) • **0**--no previous entries (only search from the present moment forward) The default is 0.

Description	How to Set It
Filtering	
Event Types	
Error	Select **Yes** to monitor Error entries. The default is Yes.
Warning	Select **Yes** to monitor Warning entries. The default is Yes.
Information	Select **Yes** to monitor Information Entries. The default is unselected.
Other	
Filter -- Source	To monitor events generated by a particular source, enter an appropriate search string. This script looks for matching entries in the Event Log's **Source** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Category	To monitor events in a particular category, such as Server or Logon, enter an appropriate search string. This script looks for matching entries in the Event Log's **Category** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Event ID	To monitor particular event IDs, enter an appropriate search string or ID range, for example, 100-2000. This script looks for matching entries in the Event Log's **Event** field. Multiple IDs and ranges can be entered, separated by commas and no spaces. For example: `1,2,10-15,202`. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- User	To monitor events associated with a particular user, enter an appropriate search string, for example, `<domain name>\<user name>`. This script looks for matching entries in the Event Log's **User** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Computer	To monitor events generated by a particular computer, enter an appropriate search string. This script looks for matching entries in the Event Log's **Computer** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Description	To monitor events with a particular detail description or containing keywords in the description, enter an appropriate search string. This script looks for matching entries in the Event Log's **Description** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Event Notification	
Raise event if new log entries found?	Select **Yes** to raise an event if new log entries are found. The default is Yes.

Description	How to Set It
Maximum number of entries per event message	Specify the maximum number of entries to be recorded into each event's detail message. If this script finds more entries from the log than can be put into one event message, it will return multiple events to report all the outstanding entries in the log. The default is 1 entry.
Event severity when new event log entries found	Set the severity level, from 1 to 40, to indicate the importance of an event in which new log entries are fund. The default is 10 (red event indicator).
Data Collection	
Collect data for number of matching entries?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of Event Log entries that match your filtering criteria. Additional information is supplied in the data detail message. The default is unselected.

EventLog (W32Time)

Use this Knowledge Script to monitor the Windows Event Log for Active Directory entries associated with the Windows Time service (`W32Time`). You can configure this script to scan the log only for entries that match a set of filtering criteria.

This script does not fully rescan the event log each time it runs. All event-log entries that match the filtering criteria are returned in the event or data point detail message.

You can restrict the types of log entries that generate an event by using the *Filtering* parameters:

- Use the *Event Type* parameters to search only certain types of events, such as Warning events.
- Use the *Other* parameters to search only for specific information, such as events associated with a specific user or computer name.

Note
Only the most recent batch of events can be viewed in the data point detail message. For example, assume you set this script to scan all previous entries in the event log and list ten matching entries in each event detail message. When the script runs, 30 entries are found that match your filtering criteria. In this case, the script would create three child events for the interval. Each child event would have ten entries: the oldest matching entries in one child event batch, the second oldest in a second batch, and the most recent in a third batch. If this same job is collecting data and you view the detail message for the interval, only the entries from the third child event (Batch 3) are displayed.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the EventLog (W32Time) job fails. The default is 35 (magenta event indicator).
Monitor Windows System log for time synchronization events	
Start with events in past	Set this parameter to control checking for the first job iteration. After the first iteration, checking of the log is incremental: • **-1**--all the existing log entries • **n**--entries from the past *n* hours (8 for the past 8 hours, 50 for the past 50 hours, etc.) • **0**--no previous entries (only search from the present moment forward) The default is 0.

Description	How to Set It
Filtering	
Event Types	
Error	Select **Yes** to monitor Error entries. The default is Yes.
Warning	Select **Yes** to monitor Warning entries. The default is Yes.
Information	Select **Yes** to monitor Information entries. The default is unselected.
Other	
Filter -- Source	To monitor events generated by a particular source, enter an appropriate search string. This script looks for matching entries in the Event Log's **Source** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Category	To monitor events in a particular category, such as Server or Logon, enter an appropriate search string. This script looks for matching entries in the Event Log's **Category** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Event ID	To monitor particular event IDs, enter an appropriate search string or ID range, for example, 100-2000. This script looks for matching entries in the Event Log's **Event** field. Multiple IDs and ranges can be entered, separated by commas and no spaces. For example: `1,2,10-15,202`. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- User	To monitor events associated with a particular user, enter an appropriate search string, for example, `<domain name>\<user name>`. This script looks for matching entries in the Event Log's **User** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Computer	To monitor events generated by a particular computer, enter an appropriate search string. This script looks for matching entries in the Event Log's **Computer** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Description	To monitor events with a particular detail description or containing keywords in the description, enter an appropriate search string. This script looks for matching entries in the Event Log's **Description** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Event Notification	
Raise event if new log entries found?	Select **Yes** to raise an event if new log entries are found. The default is Yes.

Description	How to Set It
Maximum number of entries per event message	Specify the maximum number of entries to be recorded into each event's detail message. If this script finds more entries from the log than can be put into one event message, it returns multiple events to report all the outstanding entries in the log. The default is 1 entry.
Event severity when new event log entries found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which new log entries are found. The default is 10 (red event indicator).
Data Collection	
Collect data for number of matching entries?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of Event Log entries that match your filtering criteria. Additional information is supplied in the data detail message. The default is unselected.

FSMOChange

Use this Knowledge Script to monitor changes to Flexible Single Master Operations (FSMO) roles in an Active Directory forest. This script raises an event if the domain controller for any role is changed.

Tip
Carefully monitor any FSMO role-holder movements to help correlate performance issues with improper role-holder placement.

Resource Objects

Active Directory domain

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the FSMOChange job fails. The default is 35 (magenta event indicator).
Monitor changes to FSMO roles	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).

Description	How to Set It
Event Notification	
Raise event if change to FSMO roles detected?	Select **Yes** to raise an event if changes to FSMO roles are detected. The default is Yes.
Event severity when change detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which changes to FSMO roles are detected. The default severity level is 20 (yellow event indicator).
Data Collection	
Collect data for changes to FSMO roles?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • 100 -- no change to the FSMO roles detected, or • 0 -- change to FSMO role detected. The default is unselected.

FSMOHealth

Use this Knowledge Script to monitor access to the domain controllers that have been given any Flexible Single Master Operations (FSMO) role. Operations Master roles include:

- Schema Master
- Domain Naming Master
- Primary Domain Controller (PDC) emulator
- Relative ID (RID) Master
- Infrastructure Master

This script uses the Active Directory Service Interface (ADSI) and attempts to connect to each domain controller that is serving an FMSO role. In addition, this script raises an event if the connection fails for any domain controller holding an Operations Master role. The event detail message identifies the domain controller that failed to respond and its FMSO role.

Job Delegation and the FSMOHealth Knowledge Script

The Knowledge Script job delegation feature, discussed in "AD Knowledge Script Job Delegation" on page 88, is implemented differently in this script than in other scripts. Unlike those other scripts, FSMOHealth performs a connectivity check. For obvious reasons, you do not want it merely to perform a connectivity self-check on the domain controller (DC) to which the job has been delegated.

When enabling job delegation for AD_FSMOHealth, you are not asked to select the role holder to which the monitoring job is to be delegated. Instead, this script runs on every domain FSMO role holder: the IM, PDC, and RID. If one DC in the domain holds all the roles, another DC in the domain is selected to connect to the Operations Master.

Note
Having only one DC in a domain is not a recommended Active Directory practice. Redundancy for the domain partition is recommended, and a lack of redundancy for a domain partition is identified by the replication monitoring feature of the ServerHealthKnowledge Script.

Deploying this Script Without Job Delegation

Deploy this script to one DC per domain, selecting a DC that does not hold any of the domain FSMO roles. If no such DC exists (say, if you have three or fewer DCs and each holds a domain FSMO role), then deploy this script to every DC, because they all hold a domain FSMO role and will then check each other.

Exercise care in selecting the DCs to be monitored and deploying the job to those DCs. It is a good idea to create a custom server group for this script unless you enable job delegation. If you change the domain FSMO role holders, modify the server group accordingly.

Resource Objects

Active Directory domain

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the FSMOHealth job fails. The default is 35 (magenta event indicator).
Monitor connectivity to FSMO role holders	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on each DC that holds a domain FSMO role. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes a domain FSMO role. The event indicates that the monitored computer has assumed a domain FSMO role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes a domain FSMO role. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up a domain FSMO role. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes a domain FSMO role. The default is 30 (blue event indicator).
Event Notification	
Raise event if domain controller inaccessible?	Select **Yes** to raise an event if a DC that holds a FSMO role is inaccessible. The default is Yes.
Event severity when domain controller inaccessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which a DC that holds a FSMO role is inaccessible. The default is 10 (red event indicator).
Data Collection	
Collect data for inaccessible DC and its role?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns a value of 100 if there is no change to the FMSO roles, or a value of 0 if there has been a change durng the interval. The default is unselected.

FSMOPlacement

Use this Knowledge Script to monitor the placement of a Flexible Single Master Operations (FSMO) role.

Active Directory follows Microsoft Best Practices for the placement of FSMO roles:

- The FSMO role of the infrastructure master must not host a global catalog unless all domain controllers in the domain of the Infrastructure Master are hosting global catalogs.
- The Domain-Naming Master must host a global catalog.

This script raises an event if the placement of the FSMO role violates either rule.

Resource Objects

Active Directory domain

Default Schedule

The default interval for this script is **Every 4 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the FSMOPlacement job fails. The default is 35 (magenta event indicator).
Monitor FSMO role placement	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.

Description	How to Set It
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Event Notification	
Raise event if role placement invalid?	Select **Yes** to raise an event if the FSMO role placement is invalid. The default is Yes.
Event severity when role placement invalid	Set the severity level, from 1 to 40, to indicate the importance of an event in which the FSMO role placement is invalid. The default is 10 (red event indicator).
Data Collection	
Collect data for role placement status (valid or invalid)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • 100 -- the FMSO role placement is valid, or • 0 -- a problem with role placement was found. The default is unselected.

GlobalCatalogChange

Use this Knowledge Script to monitor changes to the list of global catalog (GC) servers defined in the forest. This script raises an event if new GC servers are added or any GC servers are dropped.

Tip
Global catalog placement is critical to Active Directory health, especially in branch office deployments. Carefully monitor GC placement to ensure that clients can always log in and use Microsoft Exchange, even if a WAN link is down. Proper GC placement also prevents significant accidental WAN traffic because clients will go to remote GCs if a local GC is not present.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 4 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the GlobalCatalogChange job fails. The default is 35 (magenta event indicator).
Monitor global catalog server changes	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role (Domain Master or Schema Master) that you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate forest-wide monitoring to the	Select the server role to which the job should be delegated: **Domain Master** or **Schema Master**. The default is Domain Master.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate forest-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate forest-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.

Description	How to Set It
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Event Notification	
Raise event if global catalog server changes detected?	Select **Yes** to raise an event if GC servers are added or dropped. The default is Yes.
Event severity when changes detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which GC servers are added or dropped. The default is 25 (blue event indicator).
Data Collection	
Collect data for global catalog server changes?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • 0 -- no changes to the list of global catalog servers, or • 1 -- there have been changes to the list of global catalog servers. The default is unselected.

GlobalCatalogHealth

Use this Knowledge Script to monitor access to the global catalog (GC) servers defined in the forest. This script retrieves a list of all GC servers within the site or forest specified in the *Site list* parameter, and tries to connect to them using ADSI. In addition, this script raises an event if the connection fails for any domain controller hosting a GC.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the GlobalCatalogHealth job fails. The default is 35 (magenta event indicator).
Monitor connectivity to global catalog servers	
Scope of global catalog monitoring	Select **site(s)** or **forest** to indicate the scope within which you want to monitor your global catalog servers.
Site list (comma-separated, no spaces)	Specify a list of sites to monitor. Separate names by commas and no spaces. The list can contain no more than 4096 characters.
Full path to file with list of sites	You can use a text file that contains a list of sites, rather than the previous parameter. Specify the path to that file here. The path can be to a file on the computer where the AppManager agent is installed (for example, `C:\AMAgent\sitelist`), or a UNC path if the file exists on a different computer (for example, `\\Server1\SiteLists\sitelist`). The file should contain one site per line. The AppManager agent must have read permission for the file.
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the Inter-Site Topology Generator (ISTG) server role. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate site-wide monitoring to the	Indicates the server role to which the job should be delegated, the ISTG.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the domain controller (DC) assumes the ISTG server role. The event indicates that the monitored computer has assumed that role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the ISTG server role. The default is 30 (blue event indicator).

Description	How to Set It
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the ISTG server role. The event indicates that the monitored computer has relinquished that role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the ISTG server role. The default is 30 (blue event indicator).
Event Notification	
Raise event if connection to global catalog fails?	Select **Yes** to raise an event if the connection to the GC fails. The default is Yes.
Event severity when connection fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the connection to the GC fails. The default is 10 (red event indicator).
Data Collection	
Collect data for global catalog status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • 0 -- global catalog servers are down, or • 100 -- all global catalog servers are accessible. The script also returns the number of global catalog servers that are accessible. The default is unselected.

InboundReplStat

Use this Knowledge Script to monitor the number of inbound replication requests per second in the Active Directory. This script raises an event if the number of inbound replications per second exceeds the threshold you set.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counters
NTDS	DRA Inbound Values Total/sec
DirectoryServices	If data collection is enabled, values for the following counters are included in the data detail message: • DRA Inbound Objects Applied/sec • DRA Inbound Objects Filtered/sec • DRA Inbound Properties Applied/sec • DRA Inbound Properties Filtered/sec

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the InboundReplStat job fails. The default is 35 (magenta event indicator).
Monitor inbound replication rate	
Event Notification	
Raise event if inbound replication rate exceeds threshold?	Select **Yes** to raise an event if the inbound replication rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum inbound replication rate	Specify the maximum number of inbound replication requests allowed per second before an event is raised. The default is 120 requests per second.
Event severity when replication rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the inbound replication rate exceeds the threshold. The default is 20 (yellow event indicator).

Description	How to Set It
Data Collection	
Collect data for inbound replication rate?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total inbound replication rate per second (replication requests/sec). The default is unselected.

InterReplTraffic

Use this Knowledge Script to monitor the replication traffic from the DRA (Directory Replication Agent) between Active Directory sites, sometimes referred to as inter-site replication traffic. You specify the maximum traffic level—the number of inbound and outbound bytes per second and the number of consecutive times the threshold can be exceeded—before an event is raised. This script raises an event if either the inbound bytes per second or the outbound bytes per second exceeds the threshold for the specified consecutive number of monitoring intervals.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counters
NTDS DirectoryServices	DRA Inbound Bytes Compressed (Between Sites, After Compression)/sec DRA Outbound Bytes Compressed (Between Sites, After Compression)/sec **Note** The same threshold applies to both counters. No computation applies.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 3 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the InterReplTraffic job fails. The default is 35 (magenta event indicator).
Monitor intersite replication traffic	
Event Notification	
Raise event when threshold exceeded too often?	Select **Yes** to raise an event if the replication traffic threshold is exceeded too often. events. The default is Yes.
Threshold -- Maximum inbound or outbound bytes per second	Specify the maximum number of inbound or outbound replication bytes allowed per second before an event is raised. The default is 60000 bytes per second. Inbound bytes and outbound bytes per second are monitored separately and checked against this threshold. This script raises an event If either the inbound rate or the outbound rate exceeds this threshold more than *n* times.

Description	How to Set It
Maximum consecutive intervals threshold can be exceeded	Specify the maximum number of consecutive intervals the inbound or outbound rate can be exceeded before raising an event. The default is 1 interval. Because replication traffic can have periodic spikes, you may want to set this parameter to a higher value to filter out unnecessary events. For example, you may want to allow the inbound/outbound byte rate to exceed the threshold 3 to 4 times before an event is raised.
Event severity when replication traffic exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which replication traffic exceeds the threshold more than *n* times. The default is 20 (yellow event indicator).
Data Collection	
Collect data for inbound and outbound bytes per second?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of inbound bytes per second and the number of outbound bytes per second. The default is unselected.

IntraReplTraffic

Use this Knowledge Script to monitor the replication traffic from the DRA (Directory Replication Agent) within an Active Directory site (intrasite replication traffic). You specify the maximum number of inbound or outbound bytes per second and the number of consecutive times the threshold can be exceeded before raising an event. This script raises an event if the rate of either inbound bytes per second or outbound bytes per second exceeds the threshold for the specified consecutive number of monitoring intervals.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counters
NTDS	DRA Inbound Bytes Not Compressed (Within Site)/sec
DirectoryServices	DRA Outbound Bytes Not Compressed (Within Site)/sec
	Note The same threshold applies to both counters. No computation applies.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the IntraReplTraffic job fails. The default is 35 (magenta event indicator).
Monitor intrasite replication traffic	
Event Notification	
Raise event when threshold exceeded too often?	Select **Yes** to raise an event if the replication traffic threshold is exceeded more than *n* times. The default is Yes. Use the *Maximum consecutive intervals threshold can be exceeded* parameter to determine the value of *n*.
Threshold -- Maximum inbound or outbound bytes per second	Specify the maximum number of inbound or outbound replication bytes per second allowed before an event is raised. The default is 60000 bytes per second. The inbound bytes and outbound bytes per second are monitored separately and checked against this threshold. This script raises an event If either the inbound rate or the outbound rate exceeds this threshold more than *n* times.

Description	How to Set It
Maximum consecutive intervals threshold can be exceeded	Specify the consecutive number of intervals the inbound or outbound rate can be exceeded before raising an event. The default is 1 interval. Because replication traffic can have periodic spikes, you may want to set this parameter to a higher value to filter out unnecessary events. For example, you may want to allow the inbound/outbound byte rate to exceed the threshold 3 to 4 times before an event is raised.
Event severity when replication traffic exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the replication traffic threshold is exceeded more than *n* times. The default is 20 (yellow event indicator).
Data Collection	
Collect data for inbound and outbound bytes per second?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of inbound bytes per second and the number of outbound bytes per second. The default is unselected.

KCCConnections

Use this Knowledge Script to monitor the number of Knowledge Consistency Checker (KCC) connections to and from a domain controller. The KCC is a core Active Directory service that is responsible for generating the intersite and intrasite replication topology. This script raises an event if the number of inbound or outbound KCC connections exceeds the thresholds you set.

Significant changes in the number of replication partners indicates that something significant involved in Active Directory replication has failed, and KCC is automatically trying to recover. If the number of partners is too great, the replication window may close before replication can complete, causing replication to fail. NetIQ Corporation recommends that no domain controller should ever serve more than 50 KCC connections due to the load generated by each partner.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the KCCConnections job fails. The default is 35 (magenta event indicator).
Monitor number of KCC connections	
Event Notification	
Raise event if number of KCC connections exceeds threshold?	Select **Yes** to raise an event if the number of KCC connections exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of inbound KCC connections	Specify the maximum number of inbound KCC connections allowed before an event is raised. The default is 10 connections.
Threshold -- Maximum number of outbound KCC connections	Specify the maximum number of outbound KCC connections allowed before an event is raised. The default is 10 connections.
Event severity when either threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).
Data Collection	
Collect data for number of KCC connections?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of KCC connections. The default is unselected.

KCCDisabled

Use this Knowledge Script to check if the Knowledge Consistency Checker (KCC) is enabled or disabled for a site or server. The KCC is a core Active Directory service that is responsible for generating the intersite and intrasite replication topology. You can set this script to reenable the KCC for either intersite or intrasite replication topology if it is found to be disabled.

Note
Enabling the KCC requires Domain Admin permission. If you want to use this Knowledge Script to enable the KCC, you must set the Update Definition in User Variables. agent to run as an account with Domain Admin permission or specify an account and password with Domain Admin permission to use.

Resource Object

Active Directory domain controller where AppManager version 5.0.1 or later is installed

Default Schedule

The default interval for this script is Every hour.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the KCCDisabled job fails. The default is 35 (magenta event indicator).
Monitor KCC status	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the Inter-Site Topology Generator (ISTG) server role. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate site-wide monitoring to the	Indicates the server role to which the job should be delegated, the ISTG.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the domain controller (DC) assumes the ISTG server role. The event indicates that the monitored computer has assumed that role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the ISTG server role. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the ISTG server role. The event indicates that the monitored computer has relinquished that role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the ISTG server role. The default is 30 (blue event indicator).
Event Notification	

Description	How to Set It
Raise event if KCC is disabled?	Select **Yes** to raise an event if the KCC is disabled. The default is Yes.
Event severity when KCC is disabled	Set the severity level, from 1 to 40, to indicate the importance of an event in which the KCC is disabled. The default is 20 (yellow event indicator).
Raise event if KCC is enabled?	Select **Yes** to raise an event if the KCC is enabled. The default is unselected.
Event severity when KCC is enabled	Set the severity level, from 1 to 40, to indicate the importance of an event in which the KCC is enabled. The default is 25 (blue event indicator).
Data Collection	
Collect data for KCC status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • 100 -- KCC is enabled • 0 -- KCC is disabled. The default is unselected.
Remediation	
Enable KCC for intrasite topology generation?	Select **Yes** to reenable the KCC for intrasite topology generation if the KCC is disabled. The default is Yes.
Enable KCC for intersite topology generation?	Select **Yes** to reenable the KCC for intersite topology generation if the KCC is disabled. The default is unselected.
Account to use to enable KCC (leave blank to use the MC account)	Specify the account to be used by AppManager to reenable the KCC. Use the format `domain\user` or `user@domain`. Leave this value blank to use the managed client account.
Password for this account	Specify the password associated with the account you noted above. The maximum length allowed for the password is 32 characters.

KDCRequests

Use this Knowledge Script to monitor the rate of Kerberos Key Distribution Center (KDC) requests. The Key Distribution Center provides services for authentication and security. This script lets you set thresholds for Authentication Service (AS) requests per second and Ticket Granting Service (TGS) requests per second. In addition, this script raises an event if either threshold is exceeded.

Tip
This scripts monitors the number of authentications per second coming into the KDC. A burst indicates a surge of logon traffic.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counters
NTDS	KDC AS Requests
Security System-Wide Statistics	KDC TGS Requests

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the KDCRequests job fails. The default is 35 (magenta event indicator).
Monitor KDC request rate	
Event Notification	
Raise event if KDC request rate exceeds a threshold?	Select **Yes** to raise an event if the KDC request rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum Authentication Service request rate	Specify the maximum number of Authentication Service requests allowed per second before an event is raised. The default is 20 requests per second.
Threshold -- Maximum Ticket Granting Service request rate	Specify the maximum number of Ticket Granting Service requests allowed per second before an event is raised. The default is 20 requests per second.

Description	How to Set It
Event severity when either threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 20 (yellow event indicator).
Data Collection	
Collect data for KDC request rates?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the rate of Authentication Service and Ticket Granting Service requests (requests/ second) during the monitoring interval. The default is unselected.

NumberOfComputers

Use this Knowledge Script to monitor the number of computers in a domain or organizational unit. This script raises an event if the number of computers exceeds the threshold you set.

Resource Objects

Active Directory domain or organizational unit (OU).

To monitor OUs with this script, specify `organizationalUnit` in the *Classes to include* parameter of the Discovery_ActiveDS Knowledge Script.

When dropped on an OU, this script monitors all computers in that OU and any child OUs. The total number of computers for an OU consists of all computers in the OU and in any child OUs.

When you drop this script on a domain, the domain and all child OUs will show a job is running; however, the job runs only on the domain and not on the child OUs.

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance an event in which the NumberOfComputers job fails. The default is 35 (magenta event indicator).
Monitor number of computers	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.

Description	How to Set It
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Event Notification	
Raise event if number of computers exceeds threshold?	Select **Yes** to raise an event if the number of computers in the domain or OU exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of computers	Specify the maximum number of computers that can be in the domain or OU before an event is raised. The default is -1 computer. **Note** You must change the default setting to run this script. Collect data to establish a baseline, then specify a threshold appropriate for your environment.
Event severity when number of computers exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of computers exceeds the threshold. The default is 5 (red event indicator).
Data Collection	
Collect data for number of computers?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of computers detected during the monitoring interval. The default is unselected.
Number of computers to return when collecting data (0 for all computers)	Specify the number of computers you want returned when collecting data. For example, if you set this parameter to 500 and the domain contains 2,000 computers, only the first 500 computers are returned in the event message. Select 0 to return all computers. The default is 500 computers.

NumberOfDCs

Use this Knowledge Script to monitor changes to the number of domain controllers (DCs) in a domain, site, or forest.

The script retrieves the total number and names of all DCs using ADSI (Active Directory Service Interfaces). In addition, this script raises an event if any changes are detected during consecutive iterations. By default, only the local domain or site of the computer running this script is monitored. However, you can supply a list of fully qualified domain names or sites to monitor. The list overrides the local domain or site — that is, the domain of the local computer will not be monitored unless it is included in the list you supply.

This script also raises an event if the number of DCs falls below the minimum threshold or exceeds the maximum threshold.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the NumberOfDCs job fails. The default is 35 (magenta event indicator).
Monitor number of domain controllers	
Monitor number of DCs in:	Select the domain, site, or forest where you want to monitor the number of DCs.

List of fully qualified domains or sites to monitor (comma-separated, no spaces)	Specify a list of fully qualified domain names or sites to monitor, separated by commas and no spaces. Leave this parameter blank to use the local domain or site of the DC.
	For example, if you selected **domains** for the *Monitor number of DCs in* parameter, you could enter:
	`us.netiq.local,dev.us.netiq.local`
	If you selected sites, enter:
	`netiqus,netiqdev`

Full path to file with list of domains or sites	To instruct this script to read from a file with a list of domains or sites, rather than entering a list in the *List of fully qualified domains or sites to monitor* parameter, enter the full directory path to that file here. The path can be to a file on the computer where the AppManager agent is installed (for example, `C:\AMAgent\domainsitelist`), or a UNC path if the file exists on a different computer (for example, `\\Server1\SiteLists\domainsitelist`). The file should contain one site per line. The AppManager agent must have read permission for the file.

Description	How to Set It
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate [scope] monitoring to the...* parameter. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Delegate site-wide monitoring to the	Indicates the server role to which the job should be delegated, the ISTG.
Delegate forest-wide monitoring to the	Select the server role to which the job should be delegated: **Domain Master** or **Schema Master**. The default is Domain Master.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate [scope] monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate [scope] monitoring to the...* parameter. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to enable events if the DC gives up the server role you selected for the *Delegate [scope] monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate [scope] monitoring to the...* parameter. The default is 30 (blue event indicator).
Event Notification	
Raise event if threshold exceeded or not met?	Select **Yes** to raise an event if the number of DCs exceeds or falls below the threshold you set. The default is Yes.
Threshold -- Minimum number of domain controllers	Specify the minimum number of DCs that must exist to prevent an event from being raised. The default is 2 DCs.
Threshold -- Maximum number of domain controllers	Specify the maximum number of DCs that can exist before an event is raised. The default is 20 DCs.
Event severity when threshold exceeded or not met	Set the severity level, from 1 to 40, to indicate the importance of ant in which the number of DCs exceeds or falls below the threshold. The default is 5 (red event indicator).
Data Collection	
Collect data for number of DCs?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of DCs detected during the monitoring interval. The default is unselected.

NumberOfGCs

Use this Knowledge Script to monitor changes to the number of global catalog (GC) servers in a domain, site, or forest. If the number of servers falls below the minimum threshold or exceeds the maximum threshold you set, an event is raised.

By default, only the local domain or site of the computer running this script is monitored for changes to the number of GC servers. However, you can supply a list of fully qualified domain names or sites to monitor. The list overrides the local domain or site — that is, the domain of the local computer will not be monitored unless it is included in the list you supply.

The first time the job runs, the script retrieves the total number of, and a list of, all GC servers in a domain, site, or forest.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the NumberOfGCs job fails. The default is 35 (magenta event indicator).
Monitor number of domain controllers	
Monitor number of global catalog servers in:	Select the scope of monitoring: whether you want to monitor the number of GC servers in a domain, site, or forest.

List of fully qualified domains or sites to monitor (comma-separated, no spaces)	Specify a list of fully qualified domain names or sites to monitor, separated by commas and no spaces. Leave this parameter blank to use the local domain or site of the domain controller.
	For example, if you selected **domains** for the *Monitor number of global catalog servers in* parameter, you could enter:
	`us.netiq.local,dev.us.netiq.local`
	If you selected sites, enter:
	`netiqus,netiqdev`

Full path to file with list of domains or sites	To instruct this script to read from a file with a list of domains or sites, rather than entering a list for the *List of fully qualified domains or sites to monitor* parameter, enter the full directory path to that file here. The path can be to a file on the computer where the AppManager agent is installed (for example, `C:\AMAgent\domainsitelist`), or a UNC path if the file exists on a different computer (for example, `\\Server1\SiteLists\domainsitelist`). The file should contain one site per line. The AppManager agent must have read permission for the file.

Description	How to Set It
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate [scope] monitoring to the...* parameter. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Delegate site-wide monitoring to the	Indicates the server role to which the job should be delegated, the ISTG.
Delegate forest-wide monitoring to the	Select the server role to which the job should be delegated: **Domain Master** or **Schema Master**. The default is Domain Master.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate [scope] monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate [scope] monitoring to the...* parameter. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate [scope] monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate [scope] monitoring to the...* parameter. The default is 30 (blue event indicator).
Event Notification	
Raise event if threshold exceeded or not met?	Select **Yes** to raise an event if the number of GC servers exceeds or falls below the threshold you sent. The default is Yes.
Threshold -- Minimum number of global catalog servers	Specify the minimum number of GC servers that must exist to prevent an event from being raised. The default is 1 global catalog server.
Threshold -- Maximum number of global catalog servers	Specify the maximum number of GC servers that can exist before an event is raised. The default value is 20 global catalog servers.
Event severity when threshold exceeded or not met	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of GC servers exceeds or falls below the threshold. The default is 20 (yellow event indicator).
Data Collection	
Collect data for number of global catalog server?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of GC servers detected in the interval. The first time the job runs, it also returns a list of all the GC servers. The default is unselected.

NumberOfGroups

Use this Knowledge Script to monitor the number of groups in a domain or organizational unit. This script raises an event if the number of groups exceeds the threshold you set.

Resource Objects

Active Directory domain or organizational unit (OU)

To monitor OUs with this script, specify `organizationalUnit` in the *Classes to include* parameter of the Discovery_ActiveDS Knowledge Script.

When dropped on an OU, this script monitors all groups in that OU and any child OUs. The total number of groups for an OU consists of all groups in the OU and in any child OUs.

When you drop this script on a domain, the domain and all child OUs will show a job is running; however, when the script is dropped on a domain, the script runs only on the domain and not on the child OUs.

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the NumberOfGroups job fails. The default is 35 (magenta event indicator).
Monitor number of groups	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.

Description	How to Set It
Event severity when DC relinquishes this role	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Event Notification	
Raise event if number of groups exceeds threshold?	Select **Yes** to raise an event if the number of groups exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of groups	Specify the maximum number of groups that can be in the domain, site, or forest before an event is raised. The default is -1 group. **Note** You must change the default setting to run this script. Collect data to establish a baseline, then specify a threshold appropriate to your environment.
Event severity when number of groups exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of groups exceeds the threshold. The default is 20 (yellow event indicator).
Data Collection	
Collect data for number of groups?	Select **Yes** to collect data for charts and reports. If enabled, data collecton returns the number of groups detected during the monitoring interval. the default is unselected.
Number of groups to return when collecting data (0 for all groups)	Specify the number of groups you want returned when collecting data. For example, if you set this parameter to 400 and the domain contains 700 groups, only the first 400 groups are returned. Enter 0 to return all groups. The default is 400 groups.

NumberOfObjects

Use this Knowledge Script to monitor the number of objects in a domain or organizational unit. This script raises an event if the number of objects exceeds the threshold you set.

You should monitor the number of objects in your user domains to proactively detect any significant growth in the total number of objects. Large object growth is an unusual and serious event. Large growth overwhelms replication, causes high CPU on all affected domain controllers, and can create out-of-disk space conditions.

Tip
The recommended value for the Threshold ~ Maximum number of objects parameter is the current number of objects, plus 10% of that value.

Resource Objects

Active Directory domain or organizational unit (OU)

To monitor OUs with this script, specify `organizationalUnit` in the *Classes to include* parameter of the Discovery_ActiveDS Knowledge Script.

When dropped on an OU, this script monitors all objects in that OU and any child OUs. The total number of objects for an OU consists of all objects in the OU and in any child OUs.

When you drop this script on a domain, the domain and all child OUs will show a job is running; but, in reality, the script runs only on the domain and not on the child OUs.

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the NumberOfObjects job fails. The default is 35 (magenta event indicator).
Monitor number of objects	
Object class to check (* for all objects)	Select the type of Active Directory object to check: **domain**, **computer**, or **user**. Select an asterisk (*) to check for all objects. The default is none.
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.

Description	How to Set It
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to enable events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to enable events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Event Notification	
Raise event when number of objects exceeds threshold?	Select **Yes** to raise an event if the number of objects in the organizational unit exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of objects in class	Specify the maximum number of objects of the specified class that can be in the organizational unit before an event is raised. The default is -1 object. **Note** Change the default setting to run this script. Collect data to establish a baseline, then specify a threshold appropriate to your environment.
Event severity when number of objects exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of objects in the organizational unit exceeds the threshold. The default is 5 (red event indicator).
Data Collection	
Collect data for number of objects?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of objects detected during the monitoring interval. The default is unselected.
Number of objects to return when collecting data (0 for all objects)	Specify the number of objects you want to include when collecting data. For example, if you set this parameter to 500 and the domain contains 800 objects, only the first 500 objects are returned. Enter 0 to return all objects. The default is 500 objects.

NumberOfPrintQueues

Use this Knowledge Script to monitor the number of print queues associated with the printer objects in a domain or an organizational unit. This script raises an event if the number of printer queues exceeds the threshold you set.

Resource Objects

Active Directory domain or organizational unit (OU)

To monitor OUs with this script, specify `organizationalUnit` in the *Classes to include* parameter of the Discovery_ActiveDS Knowledge Script.

When dropped on an OU, this script monitors all print queues in that OU and any child OUs. The total number of print queues for an OU consists of all print queues in the OU and in any child OUs.

When you drop this script on a domain, the domain and all child OUs will show a job is running; however, when the script is dropped on a domain, the script runs only on the domain and not on the child OUs.

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of printer queues exceeds threshold?	Select **Yes** to raise an event if the number of printer queues exceeds the threshold you set. The default is Yes.
Collect data for number of printer queues?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of printer queues detected during the monitoring interval. The default is unselected.
Threshold -- Maximum number of printer queues	Specify the maximum number of printer queues that can be in the domain or OU before an event is raised. The default is -1 printer queue. **Note** Change the default setting to run this script. Collect data to establish a baseline, then specify a threshold appropriate to your environment.
Number of printer queues to return when collecting data	Specify the number of printer queues you want returned when collecting data. For example, if you set this parameter to 500 and the domain contains 800 printer queues, only the first 500 printer queues are returned. Enter 0 to return all printer queues. The default is 500 printer queues.
Event severity when number of printer queues exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of printer queues exceeds the threshold. The default is 5 (red event indicator).

NumberOfUsers

Use this Knowledge Script to monitor the number of users in a domain or organizational unit. This script raises an event if the number of users exceeds the threshold you set.

Resource Objects

Active Directory domain or organizational unit (OU).

To monitor OUs with this script, specify `organizationalUnit` in the *Classes to include* parameter of the Discovery_ActiveDS Knowledge Script.

When dropped on an OU, this script monitors all users in that OU and any child OUs. The total number of users for an OU consists of all users in the OU and in any child OUs.

When you drop this script on a domain, the domain and all child OUs will show a job is running; but, in reality, the script runs only on the domain and not on the child OUs.

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the NumberOfUsers job fails. The default is 35 (magenta event indicator).
Monitor number of users	
Include contacts (AppManager for AD v.6.3 or later)?	Select **Yes** to include contact objects in your count of the Number of Users. By default this script refers to security users only.
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).

Description	How to Set It
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Event Notification	
Raise event when number of users exceeds threshold?	Select **Yes** to raise an event if the number of users in an organization unit or domain exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of users	Specify the maximum number of users that can be in the domain or organizational unit before an event is raised. The default is -1 user. **Note** Change the default setting to run this script. Collect data to establish a baseline, then specify a threshold appropriate to your environment.
Event severity when number of users exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of users in the domain or organizational unit exceeds the threshold. The default is 5 (red event indicator).
Data Collection	
Collect data for number of users?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of users detected in the interval. The default is unselected.
Number of users to return when collecting data (0 for all users)	Specify the number of users you want returned when collecting data. For example, if you set this parameter to 1000 and the domain or OU contains 10,000 users, only the first 1000 users are returned. Enter 0 to return all users. The default is 1000 users.

NumberOfUsersLocked

Use this Knowledge Script to monitor the number of locked user accounts in the selected a domain or organizational unit. This script raises an event if the number of locked user accounts exceeds the threshold you set.

You can set this script to automatically unlock any accounts that are found to be locked. You can also enter a comma-separated list of accounts to be unlocked. Leave the *List of accounts to unlock* parameter blank to unlock all locked accounts.

This script includes an option to ignore user accounts that have been disabled.

Tip
If your organization experiences a large number of locked accounts, this script can automatically reset them—thereby saving the organization roughly $50 per locked-out user, according to a common industry estimate.

Resource Objects

Active Directory domain or organizational unit (OU)

To monitor OUs with this script, specify `organizationalUnit` in the *Classes to include* parameter of the Discovery_ActiveDS Knowledge Script.

When dropped on an OU, this script monitors all locked user accounts in that OU and any child OUs. The total number of locked user accounts for an OU consists of all locked user accounts in the OU and in any child OUs.

When you drop this script on a domain, the domain and all child OUs will show a job is running; however, when the script is dropped on a domain, the script runs only on the domain and not on the child OUs.

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the NumberOfUsersLocked job fails. The default is 35 (magenta event indicator).
Monitor number of locked user accounts	
Omit disabled accounts (AppManager for AD v6.2 or later)?	Select **Yes** to ignore disabled user accounts when checking for locked user accounts. By default, this script includes disabled accounts when checking for locked user accounts. **Note** This parameter is available only if you are running AppManager for Active Directory version 6.2 or later.

Description	How to Set It
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see "AD Knowledge Script Job Delegation" on page 88.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30 (blue event indicator).
Event Notification	
Raise event if number of locked user accounts exceeds threshold?	Select **Yes** to raise an event if the number of locked user accounts exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of locked user accounts	Specify the maximum number of locked user accounts that can be in the domain naming context before an event is raised. The default is 10 locked accounts.
Event severity when number of locked accounts exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of locked user accounts exceeds the threshold. The default is 5 (red event indicator).
Data Collection	
Collect data for number of locked user accounts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of locked user accounts detected in the interval. The default is unselected.
Remediation	
Unlock accounts that are locked?	Select **Yes** to automatically unlock locked user accounts. The default is unselected.
List of accounts to unlock (comma-separated; leave blank for all)	If you enabled the previous parameter, list specific user accounts to unlock, or leave the field blank to unlock all locked user accounts. Separate multiple entries with commas and no spaces. For example, to only unlock specific accounts, enter: `wolfpack,serge,elan` **Note** Use the account name as it is displayed in the Users and Computers administrative tool. The names specified will match any part of an account name.

OutboundReplStat

Use this Knowledge Script to monitor the Active Directory outbound replication rate — the number of outbound replication requests per second. This script raises an event if the total number of outbound replication requests per second exceeds the threshold you set.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counters
NTDS	DRA Outbound Values Total/sec
DirectoryServices	If data collection is enabled, values for the following counters are included in the data detail message: • DRA Outbound Objects/sec • DRA Outbound Properties/sec

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OutboundReplStat job fails. The default is 35 (magenta event indicator).
Monitor outbound replication rate	
Event Notification	
Raise event if outbound replication rate exceeds threshold?	Select **Yes** to raise an event if the outbound replication rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum outbound replication rate	Specify the maximum number of outbound replication requests allowed per second before an event is raised. The default is 120 requests per second.
Event severity when outbound replication rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the outbound replication rate exceeds the threshold. The default is 20 (yellow event indicator).
Data Collection	
Collect data for outbound replication rate?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total outbound replication requests per second. The default is unselected.

PropertyWatch

Use this Knowledge Script to monitor changes to any property of any Active Directory object. This script raises an event if any Active Directory property changes for an object, and if Active Directory properties are not found or are not available.

This script monitors one property at a time. By default, it monitors the `whenChanged` property, which includes any changes to the Active Directory object.

Because there are many different types of Active Directory object properties, some properties are not supported by this script. If you try to monitor a property that is not supported by this script, the job fails and an event is raised.

Resource Objects

Any Windows computer

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the PropertyWatch job fails. The default is 35 (magenta event indicator).
Monitor property changes for an object	
LDAP path to the Active Directory object	Specify the LDAP path to the Active Directory object. For example: `LDAP://dc1.netiq.com/CN=Administrator,CN=Users, DC=dc1,DC=netiq,DC=com`
Active Directory property name	Specify the name of the Active Directory property you want to monitor for changes. The default is **whenChanged**. Some valid property names include: • **is Deleted**, which indicates whether the object has been deleted. • **modifyTimeStamp**, which indicates whether the object's modification time has changed. • **USNChanged**, which indicates whether the object's Update Sequence Number has changed. • **whenCreated**, which indicates when the object was created. • **allowedChildClasses**, which lists the classes that can be created under the object. • **displayName**, which indicates the object's displayed name. For example, to monitor changes to the modification time stamp for an object, specify the `modifyTimeStamp` property name. The `USNChanged` property provides similar information but uses the USN rather than a timestamp and can be useful for monitoring replicated object properties.

Description	How to Set It
Event Notification	
Raise event if object property has changed?	Select **Yes** to raise an event if the object property changes. The default is Yes.
Event severity when object property has changed	Set the severity level, from 1 to 40, to indicate the importance of an event in which the object property changes. The default is 20 (yellow event indicator).
Data Collection	
Collect data for changes to object property?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • 100 -- no property changes detected, or • 0 -- a property has changed. The default is unselected.

ReadStat

Use this Knowledge Script to monitor the Active Directory read rate — the number of Active Directory reads per second. This script raises an event if the read rate exceeds the threshold you set.

If you use this script to collect data, you have three options for what is included in the data stream and data detail message:

- One data stream that records the total read rate. The data detail message describes the percentage of Active Directory reads that are being performed by various services, such as `DRA`, `KCC`, `LSA`, `NSPI`, `SAM`, `XDS` (Windows 2000 Server), `NTDSAPI` (Windows Server 2003 and Windows Server 2008), and others.
- One data stream that records the total read rate, but without the detail message breakdown
- Seven data streams that track the total number of reads per second and the number of reads per second for various services independently. Independent data streams for the read rate of the `DRA`, `KCC`, `LSA`, `NSPI`, `SAM`, `XDS` (Windows 2000 Server), and `NTDSAPI` services (Windows Server 2003 and Windows Server 2008).

If you collect data, keep in mind that the more data streams and details you collect, the greater the impact on your database management system and overall system performance. For example, if you choose the third data collection option, you may want to adjust your archive policies or check the size of data tables in the AppManager repository more frequently.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counters
NTDS DirectoryServices	For monitoring, only the following counter is used to determine whether the threshold has been crossed and an event should be raised: • DS Directory Reads/sec If data collection is enabled and data collection mode 1 or 3 is specified, values for the following counters are included in the data detail message: • DS % Reads from DRA • DS % Reads from KCC • DS % Reads from LSA • DS % Reads from NSPI • DS % Reads from SAM • DS % Reads from XDS (Windows 2000 Server) • DS % Reads from NTDSAPI (Windows Server 2003 and Windows Server 2008)

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ReadStat job fails. The default is 35 (magenta event indicator).
Monitor rate of read operations	
Event Notification	
Raise event if read rate exceeds threshold?	Select **Yes** to raise an event if the read rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum reads per second	Specify the maximum number of Active Directory reads allowed per second before an event is raised. The default is 1 read per second.
Event severity when read rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the read rate exceeds the threshold. The default is 20 (yellow event indicator).
Data Collection	
Collect data for read rate?	Select **Yes** to collect data for charts and reports. If enabled, specify a value in the *Data collection mode* parameter. The default is unselected.
Data collection mode	Specify the type of data you want to collect. The following entries are valid: • **1** -- one data stream that records the total read rate. The data detail message describes the percentage of Active Directory read operations that are performed by various Active Directory services. • **2** -- one data stream that records the total read rate without any detail message. • **3** -- seven data streams: total read rate for all Active Directory services, and one data stream for each of 6 separate services. The default is 1 (one data stream and detail message).

ReplEventLog

Use this Knowledge Script to periodically scan the Directory Service log for Active Directory replication errors. This script raises an event if any Active Directory replication errors are found.

During the first monitoring interval, the value you specify for the *Directory Service log entries to scan* parameter determines how far back in the log to check for matching entries. As the script continues to run at subsequent intervals, it checks for any new entries created since the last time the log was checked.

You can further restrict the types of log entries that raise an event by using the *Filtering* parameters:

- Use the *Event Type* parameters to search only certain types of events, such as Warning events.
- Use the *Other* parameters to search only for specific information, such as events associated with a specific user or computer name.

Each time this script runs, it checks the Directory Service log for entries matching your selection criteria and raises an event if matching entries are found. The event detail message returns the text of the log entries found. When this script is set to collect data, it returns the number of log entries found, and the data point detail message returns the text of the log entries.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ReplEventLog job fails. The default is 35 (magenta event indicator).
Monitor Directory Service log for replication events	
Raise event if matching log entries found?	Select **Yes** to raise an event if log entries are found that match the filters you set. The default is Yes.
Start with events in past	Set this parameter to control checking for the first interval, after which, checking is incremental: • **-1**--all the existing entries • **n**--the past *n* hours (8 for the past 8 hours, 50 for the past 50 hours, etc.) • **0**--no previous entries (only search from this moment on) The default is 0.
Filtering	
Event Types	
Error	Select **Yes** to monitor Error entries. The default is Yes.
Warning	Select **Yes** to monitor Warning entries. The default is unselected.
Information	Select **Yes** to monitor Information entries. The default is unselected.
Success Audit	Select **Yes** to monitor Success Audit entries. The default is unselected.
Failure Audit	Select **Yes** to monitor Failure Audit entries. The default is unselected.
Other	
Filter -- Category	To monitor events in a particular category, such as Server or Logon, enter an appropriate search string. This script looks for matching entries in the Directory Service Log's **Category** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Event ID	To monitor particular event IDs, enter an appropriate search string or ID range, for example 100-2000. This script looks for matching entries in the Directory Service Log's **Event** field. Multiple IDs and ranges can be entered separated by commas. For example: `1,2,10-15,202` The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- User	To monitor events associated with a particular user, enter an appropriate search string, for example, `DomainName\UserName`. This script looks for matching entries in the Directory Service Log's **User** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.

Description	How to Set It
Filter -- Computer	To monitor events generated by a particular computer, enter an appropriate search string. This script looks for matching entries in the Directory Service Log's **Computer** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Description	To monitor events with a particular detail description or containing keywords in the description, enter an appropriate search string. This script looks for matching entries in the Directory Service Log's **Description** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Event Notification	
Maximum number of entries per event message	Set the maximum number of Directory Service log events that can be returned in each event report. For example, if this value is set to 30 and 67 Directory Service log events are found, then three event reports are raised: two reports containing 30 events and one report containing seven events. The Message column on the **Events** tab in the Operator Console displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration. The default is 1 entry.
Event severity when new log entries found	Set the severity level, from 1 to 40, to indicate the importance of an event in which new log entries are found. The default is 10 (red event indicator).
Data Collection	
Collect data for number of matching entries found?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of Directory Service Log entries that match your filtering criteria. Additional information is supplied in the data detail message. The default is unselected.

ReplicationCheckByUSN

Use this Knowledge Script to monitor Active Directory replication by checking Update Sequence Numbers (USN). This script checks whether replication is occurring by comparing the domain controller's update sequence number at each interval with its value during the previous monitoring interval.

If the highest USN on the local domain controller has not been incremented between iterations, it is likely that replication is not proceeding properly, and an event is raised. Because multimaster replication among peer domain controllers is such an important part of Active Directory, you should set the job interval to run this script at least every five to ten minutes in more active organizations where you make more frequent changes to Active Directory objects. If the job interval is too short, for example running every few seconds, you might raise false events.

Note
To use this script, specify server in the Classes to include parameter of the Discovery_ActiveDS Knowledge Script.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ReplicatonCheckByUSN job fails. The default is 35 (magenta event indicator).
Monitor Active Directory replication by USN	
Event Notification	
Raise event if USN not incremented?	Select **Yes** to raise an event if the USN has not incremented since the last monitoring interval. The default is Yes.
Event severity when USN not incremented	Set the severity level, from 1 to 40, to indicate the importance of an event in which the USN has not incremented since the last monitoring interval. The default is 5 (red event indicator).
Data Collection	
Collect data for replication status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns • 100 -- replication is successful, or • 0 -- the USN has not been updated and replication appears to be stale The default is unselected.

ReplicationLatency

Use this Knowledge Script to monitor Active Directory replication latency. Replication latency represents the amount of time a change made to an Active Directory partition takes to be reflected on another domain controller.

Replication latency is a significant metric in most typical service level agreements (SLAs) for Active Directory. To end-users, replication latency represents the maximum amount of time they have to wait after the Help Desk makes a requested change, such as a password reset. For example, an IT organization might want new user accounts or password resets to take effect a maximum of 30 minutes after the service-desk personnel initiate the change. This script can help you measure such service-level goals, despite the challenge of measuring replication latency through all the paths it can take.

For an environment with fewer than 30 domain controllers, it is reasonable to allow this script to periodically inject a small change in the Active Directory partitions representing every DC and measure how long it takes to replicate that change to other DCs. For environments with thousands of DCs, this script allows even these large Active Directory topologies to get replication latency data with virtually no data overhead. For more information, see "Examples of How this Script Is Used: Example 1" on page 167.

This script measures the time it takes to replicate a change from Point A to Point B and compares that amount of time to the thresholds you set. Changes are injected to the replication object by updating an object property. You can set parameters to determine where to store this data, what user authentication credentials to use, and how often to inject changes to check latency.

The script defines two roles: the *Injector*, which makes the change, and the *Monitor*, which waits for the replication data to arrive. A single domain controller can be both an Injector and a Monitor, but if you define one DC as an Injector, you need to drop this script on a second DC and designate it as the Monitor. The script injects a very tiny change to one object in a location you select. Every script interval, the script checks the selected folder and computes latency by reading every object and doing the following calculation:

```
Latency = Arrival time - Injection time
```

Based on the thresholds you set, this script raises an event based on the result of this calculation.

Injection frequency is determined by both the schedule and the value you set for the *Change injection frequency* parameter. For example, if this script runs every 17 minutes and the *Change injection frequency* is 24, a change is injected every 408 minutes (or every 24 job iterations).

If you choose to collect data, make sure you enable the appropriate *Collect data for...* parameter on a computer serving in the Monitor role or serving as both Injector and Monitor.

Resource Objects

Active Directory domain controller.

Default Schedule

The default interval for this script is **Daily schedule, Every 17 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ReplicationLatency job fails. The default is 35 (magenta event indicator).
Authenticate using alternate credentials?	Select **Yes** to use an alternative username and password for creating and accessing a container to test replication latency.
Username	Specify the username of the alternative account. Use the following format: `[domain name]\[username]` Leave blank to use the AppManager agent account.
Password	Specify the password of the alternative account. Leave blank to use the AppManager agent password.
Monitor Active Directory replication latency	
Role	Select the role of the server where you dropped the script: **Injector**, **Monitor**, or **Both**. The default is Both. The role you select determines whether the server injects changes, monitors for changes (and measures latency), or does both. The Injector can inject changes to domain, configuration, and application partitions. If you select Injector or Monitor, you should at minimum run the job on one server acting as an Injector and a second server acting as a Monitor. If you select Both, run the job on a minimum of two servers. Run this script on multiple servers to properly monitor replication latency.
Change injection frequency	Enter a value, from 1 to 360, to determine how frequently changes are injected to test replication latency, the number of monitoring intervals between injections. The value you enter is a divisor of the interval you selected on the **Schedule** tab. For example, the default schedule for this script is Every 17 minutes (Daily schedule). With this schedule, if you enter 24 for this parameter, a change is injected every 408 minutes. The default is one change for every 24 monitoring intervals. **Note** This parameter is only applicable when you select **Injector** or **Both** for the *Role* parameter.
Monitor changes from servers that are	Select the type of servers to monitor for changes: **Intersite**, **Intrasite**, or **Both**. The default is Both.
Partitions	
Change/monitor domain partition?	Select **Yes** to monitor the domain partition. The default is Yes.
Change/monitor configuration partition?	Select **Yes** to monitor the configuration partition. The default is unselected.
Change/monitor application partitions?	Select **Yes** to monitor application partitions. The default is Yes.
Monitor global catalog partitions?	Select **Yes** to monitor global catalog partitions. The default is Yes.

Description	How to Set It

Path to container relative to partition root	Specify any location where the container should be created. By default, the container is created in the root of the partition.
	For example, say the domain of the domain controller is `company.local`. If you set this parameter to `CN=AppManager` and enabled monitoring of domain and configuration partitions, the domain partition path would be:
	`CN=AppManager,DC=company,DC=local`
	and the configuration partition path would be:
	`CN=AppManager,CN=configuration,DC=company,DC=local`

Container name	Supply a name for a container that will be created in each of the partitions you selected for monitoring above. **Note** You can specify a parent container; however, you must first have created that parent container, with the appropriate security rights to allow creation of sub-objects using the credentials of the AppManager agent (by default) or the credentials you specified for the *Username* and *Password* parameters. The default container name is `AMReplicationLatencyObjects`.
Event Notification	
Raise event if latency threshold exceeded?	Select **Yes** to raise an event if the amount of intersite replication latency exceeds the threshold you set. The default is Yes.
Threshold -- Maximum intersite latency	Specify the maximum amount of intersite replication latency that can be measured before an event is raised. The default is 540 minutes.
Threshold -- Maximum intrasite latency	Specify the maximum amount of intrasite replication latency that can be measured before an event is raised. The default is 15 minutes.
Event severity when latency exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which intersite or intrasite latency exceeds the thresholds you set. The default is 10 (red event indicator).
Raise event if time skew detected?	Select **Yes** to raise an event if the creation time of an object used for replication latency monitoring appears to be earlier than the time of the corresponding monitoring job. The default is Yes. **Note** If you notice this event, verify that the report servers are synchronized to a common time source.
Event severity when time skew detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which object creation time is out of sync with the monitoring job.The default is 10 (red event indicator).
Raise event if object not updated within threshold time?	Select **Yes** to raise an event if an object is not updated within the threshold interval, which indicates that replication is not occurring. The default is Yes. **Note** If you stop a server from injecting changes, delete the replication objects that represent it.
Threshold -- Maximum time for object to be updated	Specify the maximum amount of time that can be taken for an object update to be completed before an event is raised. The default is 24 hours.
Event severity when object not updated within threshold time	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the time it takes to update an object exceeds the threshold. The default is 10.
Data Collection	

Description	How to Set It
Collect data for replication latency?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the replication latency in minutes. The default is unselected. If enabled, data streams are generated indicating the latency of the injected objects for all of the selected partitions to be monitored. **Note** This parameter is only valid if you selected **Monitor** or **Both** for the *Role* parameter.
Collect data for lost data due to latency?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of lost changes. The default is unselected.

Examples of How this Script Is Used: Example 1

You have an Active Directory forest named `company.local`. It contains the server `cdc1.company.local` (the primary domain controller and global catalog server) and `cdc2.company.local` (the secondary domain controller). This forest also contains a child domain named `sales.company.local`, which has the domain controllers `scdc1.sales.company.local` and `scdc2.sales.company.local`.

To use the ReplicationLatency script to verify that replication is occurring among all the domain controllers (DCs) in this forest, you could run it on all of the DCs listed above, designating each one as "Both" Injector and Monitor for the *Role* parameter. You could set the schedule and the *Change injection frequency* parameter so that Active Directory data would be injected at each monitoring interval into each of the partition types selected.

Acting as the Injector, each DC creates a lightweight replication object, a contact object, in each selected, writeable partition. The replication object is created in the container specified by the *Container name* and *Path to container relative to partition root* parameters.

If the container for the replication objects does not exist on the local partition, the DC attempts to create the container on a DC that hosts a writeable copy of the partition. The replication object is not created locally until the container is replicated to the local partition.

At every injection interval, the Injector changes the "`description`" property of the replication object. The timestamp of the change on the Injector (Injection time) is stored in the `description` property. Active Directory replication propagates the change to DCs that host a copy of the partition.

Acting as the Monitor, the DC checks the local container specified by the *Container name* and *Path to container relative to partition root* parameters for replication objects, created and changed by each Injector. As the Monitor, it computes the latency by measuring the difference between the Arrival time (the "`whenChanged`" property) and the Injection time for each replication object.

Examples of How this Script Is Used: Example 2

Instead of running the ReplicationLatency script with the default setting, which places target servers in the roles of both Injector and Monitor, you could run the script on pairs of Active Directory servers. You could drop it on the domain controllers `scdc1.sales.company.local` and `scdc2.sales.company.local`, designating one DC in each pair as an Injector and the other as a Monitor.

You would then enable data collection on the Monitor in each pair to measure replication latency. You would need to do the same thing for the pair `cdc1.company.local` and `cdc2.company.local`.

Examples of How this Script Is Used: Example 3

Extending the example introduced in "Examples of How this Script Is Used: Example 1" on page 167 to a very large Active Directory topology, the ReplicationLatency script could be used to selectively inject changes at a few key sites, while measuring changes at all the remote sites.

Suppose there are two main company sites, Corporate and Sales, where Help Desk personnel routinely handle user account and password resets. In addition, there are several thousand branch office sites, parts of a department store chain. A single DC from the Corporate site and one from the Sales site would act as both Injector and Monitor. Then a single DC from each of the branch office sites would run as a Monitor. This configuration would ensure that replication latency remained below the threshold you specified and would also cover the entire Active Directory topology, while minimizing the number of event notifications and the amount of collected data.

To isolate replication latency monitoring to intersite replication, you can deploy the ReplicationLatency script to a bridgehead server at each Injector and Monitor site.

ReplQueueLen

Use this Knowledge Script to monitor the queue length for unprocessed Active Directory replication synchronization requests. This script helps you to determine if replication synchronization requests are processed in a timely manner. In addition, this script raises an event if the unprocessed replication request queue length exceeds the threshold you set.

Replication queue length is a corollary indicator that replication is falling behind. It is standard to see one queue entry per partition. If this standard is exceeded, you should find out why replication is falling behind. Common causes include:

- the replication interval is too slow
- a WAN link is down
- a bridge is down (indicating a bridgehead server problem)

It is common for a bridgehead server to have many replication partners.

Tip
When setting a threshold value for the Maximum unprocessed requests in the queue parameter, try counting the number of partitions you have, add 2 (one for the schema partition and one for the configuration partition), then double the number and use the result as your threshold value.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counter
NTDS DirectoryServices	DRA Pending Replication Synchronizations

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ReplQueueLen job fails. The default is 35 (magenta event indicator).
Monitor replication synchronization request queue	
Event Notification	

Description	How to Set It
Raise event if queue length exceeds threshold?	Select **Yes** to raise an event if the length of the replication queue exceeds the threshold you set. The default is Yes.
Threshold -- Maximum unprocessed requests in queue	Specify the maximum number of replication synchronization requests that can be pending in the queue before an event is raised. The default is 12 queued requests.
Event severity when queue length exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the length of the replication queue exceeds the threshold. The default is 20 (yellow event indicator).
Data Collection	
Collect data for replication request queue length?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of pending synchronization requests. The default is unselected.

ReplSysVol

Use this Knowledge Script to monitor SysVol folder replication. This script raises event if a stale Active Directory replication is found.

Each time this script runs, it creates a text file under the SysVol directory on the target computer. It changes the file contents at consecutive job iterations and checks whether the changes are successfully replicated on replication partners. If the changes are not replicated successfully, the file content on the replication partners is considered stale.

This script can also validate the file size and the file content for all files under the SysVol folder on the replication partners. If you enable the *Discover all files that do not match file content?* parameter, all files are validated for size and content.

Notes

Validating file contents can significantly increase network traffic volume. The Perform file content validation? parameter is disabled by default. To perform this validation, this script first does some checking, and if the file sizes of the files being compared match, which is expected when the File Replication Service (FRS) replication is occurring normally, the files are read in entirety to generate a cyclic reduncancy check (CRC). Assuming FRS replication is occurring and all files are in sync, significant network traffic will probably be generated.

In some cases, the impact will be minor; the total SysVol file size for a given domain may not be very large, your network may be configured such that it can easily handle the extra traffic, or you may have set the Site option parameter to Intrasite, which disables off-site network traffic for this job. In all cases, however, you should carefully assess the likely network traffic cost of enabling file content validation before enabling this option in a production environment.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ReplSysVol job fails. The default is 35 (magenta event indicator).
Monitor SysVol replication	
Site option	Select the type of replication monitoring you want the script to perform: **Intrasite**, **Intersite**, or **Both**. The default is Both.
File comparison and validation	

Description	How to Set It
Compare files on replication partners?	Select **Yes** to compare SysVol folders. If enabled, returns the number and names of files that are not present on the replication partners. The default is unselected.
Perform file size comparison?	Select **Yes** to compare the SysVol file sizes on the monitored computers. If enabled, returns the number and names of files whose size is not consistent on the replication partners. The default is unselected.
Perform file content validation?	Select **Yes** to compare the contents of monitored SysVol folders. If enabled, returns the number and names of files whose content is not consistent on the replication partners. The default is unselected. **Warning** Enabling this option can significantly increase network traffic in the monitored domains. See the Warning in the Knowledge Script description.
Discover all files that do not match file content?	Select **Yes** to perform validation of file size and content for all SysVol files on the replication partners. The default is unselected.
Event Notification	
Raise event if stale replication found?	Select **Yes** to raise an event if replication fails and the file contents are stale. The default is Yes.
Event severity when replication fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which replication fails and the file contents are stale. The default is 5 (red event indicator).
Data Collection	
Collect data for SysVol replication status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • 1 -- SysVol replication status is up, or • 0 -- SysVol replication status is down The default is unselected.

ReportADSI_ADObjects

Use this Knowledge Script to summarize the properties and related values of objects in an Active Directory domain. The report contains information for the selected organizational unit or common name object and for all sub-objects.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Select OU or CN name	Click **Browse [...]** to select the organizational unit or common name object for which you want to create a report.
Report Settings	
Include table of parameter values?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is unselected. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The default is unselected. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Select **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Omit property when value not found?	Select **Yes** to omit any properties that do not have a value specified. The default is Yes.
Event Notification	
Raise event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is unselected.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).

Description	How to Set It
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated, but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

ReportADSI_GroupMembership

Use this Knowledge Script to create a list of all the members that belong to an Active Directory group. The report contains information for the selected organizational unit or common name object and for all sub-objects.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Select OU or CN name	Click **Browse [...]** to select the organizational unit or common name object for which you want to create a report.
Report Settings	
Include table of parameter settings?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is unselected.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is unselected. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The default is unselected. The timestamp is made up of the date and time the report was generated. A timestamp let you run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Select **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).

Description	How to Set It
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

ReportADSI_LocalService

Use this Knowledge Script list the services running on a managed computer in an Active Directory domain.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Target computer	Click **Browse [...]** to select the computer whose Active Directory services the report will list.
Report Settings	
Include table of parameter settings?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is unselected. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The default is unselected. The timestamp is made up of the date and time the report was generated. A timestamp let you run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Select **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).

Description	How to Set It
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

ReportADSI_LocalUser

Use this Knowledge Script list the local user accounts on a managed computer in an Active Directory domain.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Target computer	Click **Browse [...]** to select the computer that is the subject of your report.
Report Settings	
Include table of parameter settings?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is unselected. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The default is unselected. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Select **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).

Description	How to Set It
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

ReportADSI_ReplicationLatency

Use this Knowledge Script to report on Active Directory replication latency. This script summarizes the average, maximum, and minimum values of the data streams collected by the AD_ReplicationLatency Knowledge Script, or another script you select, within the time range you select.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse [...]** to select the computers for your report.
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Aggregation interval	Select the time interval by which the data in your report is aggregated. Possible values range from 1 to 90 hours. The default is 1 hour.
Report Settings	
Include table of parameter settings?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include table?	Select **Yes** to include a table of data stream values in the report. The default is Yes.
Include chart?	Select **Yes** to include a chart of data stream values in the report. The default is unselected.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Series style (Average)	Select a graphical style for the average value series in the chart. The default value is Line.
Chart title	Enter a title to assign to the chart of values.
Select output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is unselected. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Click **Browse [...]** to set report properties as desired.

Description	How to Set It
Add timestamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The default is unselected. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

ReportADSI_ReplSysVol

Use this Knowledge Script to display information about the consistency of files in the SysVol folder of the Report agent's corresponding domain controller and the files in the SysVol folders of any replication partners of that domain controller.

You can return a list of all files whose content does not match.

The report lists each replication partner, and for each partner, the following columns of information:

- **File Compare**. If all files in the SysVol folder also exist on the replication partner, a value of `OK` is displayed in this column. Any files that exist in the SysVol folder but do not exist on the replication partner are listed here.
- **File Size Match**. If all matching files in the SysVol folder and the replication partner's SysVol folder match in size, a value of `OK` is displayed in this column. Any files with a disparity in size are listed here.
- **File Content Match**. If you enable the *Discover all files that do not match file content* parameter and all files match for content, a value of `OK` is displayed in this column. If any files do not match for content, those files are listed here.

  If you disable the *Discover all files that do not match file content* parameter and all files match for content, a value of `OK` is displayed in this column. If a non-matching file is found, comparison of file content stops with that file, and a value of `Testing Stopped` is displayed in this column.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Discover all files that do not match file content?	Select **Yes** to return a list of all files in the replication partner's SysVol folder whose content is different than the content of matching files in the SysVol folder of the Report Agent's corresponding domain controller. The default is Yes.
Report Settings	
Include table of parameter settings?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is unselected. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.

Description	How to Set It
Add timestamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The default is unselected. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Select **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

ReportADSI_ServerRoles

Use this Knowledge Script to display the Active Directory roles for each server in the forest. Active Directory roles include FSMO, Global Catalog, Bridgehead, and Inter-Site Topology Generator.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Include forest domain naming master?	Select **Yes** to include the forest domain naming master in the report. The default is Yes.
Include forest schema master?	Select **Yes** to include the forest schema master in the report. The default is Yes.
Include domain infrastructure masters?	Select **Yes** to include domain infrastructure masters in the report. The default is Yes.
Include domain PDC emulators?	Select **Yes** to include domain PDC emulators in the report. The default is Yes.
Include domain RID masters?	Select **Yes** to include domain RID masters in the report. The default is Yes.
Include global catalogs?	Select **Yes** to include global catalogs in the report. The default is Yes.
Include bridgeheads?	Select **Yes** to include bridgeheads in the report. The default is Yes.
Include Inter-Site Topology Generators (ISTG)?	Select **Yes** to include Inter-Site Topology Generators in the report. The default is Yes.
Report Settings	
Include table of parameter settings?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is unselected. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The default is unselected. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output.

Description	How to Set It
Include Error Table?	Select **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

ReportADSI_UserAccountsDisabled

Use this Knowledge Script to generate a report listing disabled and locked accounts in an Active Directory domain. The report contains information for the selected organizational unit or common name object and for all sub-objects.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select OU or CN name	Click **Browse [...]** to select the organizational unit or common name object for which you want to create a report.
Select object classes	Indicates the object classes to include for the selected organizational unit or common name object. The default is computer and user.
Report Settings	
Include table of parameter settings?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is unselected. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The default is unselected. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Select **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).

Description	How to Set It
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

ReportADSI_UserBadPasswordCount

Use this Knowledge Script to list the number of failed logins due to bad passwords for accounts in an Active Directory domain. You can set a threshold for the maximum number of login failures due to bad passwords. Any account that exceeds the threshold you set is included in the report. The report contains information for the selected organizational unit or common name object and for all sub-objects.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Select OU or CN name	Click **Browse [...]** to select the organizational unit or common name object for which you want to create a report.
Select object classes	Indicate the object classes to include for the selected organizational unit or common name object. The default is computer and user.
Threshold -- Maximum number of login failures due to bad passwords	Specify a threshold for the number of login failures due to bad password attempts. Any user account that exceeds this threshold is included in the report. The default is 0.
Report Settings	
Include table of parameter settings?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is unselected. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The default is unselected. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Select **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.

Description	How to Set It
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

ReportADSI_UserMemberOfMoreThanOneGroup

Use this Knowledge Script to list the number of members that belong to more than one group in an Active Directory domain. The report contains information for the selected organizational unit or common name object and for all sub-objects.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Select OU or CN name	Click **Browse [...]** to select the organizational unit or common name object for which you want to create a report.
Select object classes	Indicates the object classes to include for the selected organizational unit or common name object. The default is computer and user.
Report settings	
Include table of parameter settings?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is unselected. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The default is unselected. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Select **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).

Description	How to Set It
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

ReportADSI_UserPasswordExpired

Use this Knowledge Script to list the number of accounts with expired passwords in an Active Directory domain. The report contains information for the selected organizational unit or common name object and for all sub-objects.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Select OU or CN name	Click **Browse [...]** to select the organizational unit or common name object for which you want to create a report.
Select object classes	Indicate the object classes to include for the selected organizational unit or common name object. The default is computer and user.
Report Settings	
Include table of parameter settings?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. The default is unselected. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The default is unselected. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Select **Yes to** include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).

Description	How to Set It
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

ResponseTime

Use this Knowledge Script to monitor the time it takes for the target computer to connect to and read the properties of a specific object on an Active Directory domain controller. This script raises an event if the connection or read time exceeds the threshold you set.

Increases in response time may indicate problems in Active Directory configuration.

Tip
Review response-time charts regularly to determine whether response time is trending as expected. Failure to monitor response time can lead to a wide range of problems, including very slow login times and Exchange timeouts.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ResponseTime job fails. The default is 35 (magenta event indicator).
Monitor connection and read response times	
LDAP path to object on target domain controller	Enter the LDAP path to an object on the target Active Directory domain controller. The default is `LDAP://server.netiq.com/RootDSE`.
Object property to read	Specify a property of the above object that you want Active Directory to read. Valid properties depend on the object you are requesting. The default is `serverName`.
Event Notification	
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if response time exceeds the threshold you set. The deault is Yes.
Threshold -- Maximum connection time	Specify the maximum number of milliseconds allowed to connect to the Active Directory domain controller before an event is raised. The default is 1000 milliseconds.
Threshold -- Maximum read time	Specify the maximum number of milliseconds allowed to read the property value before an event is raised. The default is 1000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which response time exceeds the threshold. The default is 15 (yellow event indicator).

Description	How to Set It
Data Collection	
Collect data for response times?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns two data streams, one for the connection time and one for the read time. The default is unselected.

SearchStat

Use this Knowledge Script to monitor the number of Active Directory search operations per second. If the search rate exceeds the threshold you set, an event is raised.

If you use this script to collect data, use the *Data collection mode* parameter to choose what is included in the data stream and data detail message:

- One data stream that records the total search rate. The data detail message describes the percentage of Active Directory searches that are being performed by various services, including `DRA`, `KCC`, `LDAP`, `LSA`, `NSPI`, `SAM`, `XDS` (Windows 2000 Server), `NTDSAPI` (Windows Server 2003 and Windows Server 2008), and others.
- One data stream that records the total search rate, but without the detail message breakdown.
- Data streams that track the total number of searches per second and the number of searches per second for various services independently. Independent data streams for the search rate of `DRA`, `KCC`, `LDAP`, `LSA`, `NSPI`, `SAM`, `XDS` (Windows 2000 Server), and `NTDSAPI` services (Windows Server 2003 and Windows Server 2008).

If you collect data, keep in mind that the more data streams and detail you collect, the greater the impact on your database management system and overall performance. For example, if you choose the third data collection option, you may want to adjust your archive policies or increase the frequency at which you check the size of Data tables in the AppManager repository.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counters
NTDS DirectoryServices	For monitoring, only the following counter is used to determine whether the threshold has been crossed and an event should be raised: • DS Directory Searches/sec If data collection is enabled and data collection mode 1 or 3 is specified, values for the following counters are included in the data detail message: • DS % Searches from DRA • DS % Searches from KCC • DS % Searches from LDAP • DS % Searches from LSA • DS % Searches from NSPI • DS % Searches from SAM • DS % Searches from XDS (Windows 2000 Server) • DS % Searches from NTDSAPI (Windows Server 2003 and Windows Server 2008)

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SearchStat job fails. The default is 35 (magenta event indicator).
Monitor rate of search operations	
Event Notification	
Raise event if search rate exceeds threshold?	Select **Yes** to raise an event if the number of search operations per second exceeds the threshold you set. The default is Yes.
Threshold -- Maximum search rate	Specify the maximum number of Active Directory search operations allowed per second before an event is raised. The default is 1 search per second.
Event severity when search rate exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of search operations per second exceeds the threshold. The default is 20 (yellow event indicator).
Data Collection	
Collect data for search rate?	Select **Yes** to collect data for charts and reports. If you enable data collection, specify the data collection mode to use in the *Data collection mode* parameter. The default is unselected.
Data collection mode	Specify the type of data you want to collect. The following entries are valid: • **1** -- one data stream that records the total search rate (searches/second). The data detail message describes the percentage of Active Directory search operations that are performed by various services. • **2** -- one data stream that records the total search rate without any detail message. • **3** -- eight data streams: total search rate for all Active Directory services, and one data stream for each of 7 separate services. The default is 1 (one data stream and detail message).

ServerHealth

Use this Knowledge Script to monitor the health of an Active Directory domain controller.

By default, this script checks to see if essential Active Directory services are installed and/or running. You can also monitor the optional DNS server service, and you can disable monitoring of any essential service.

This script using the WMI (Windows Management Instrumentation) replication provider service to check for error conditions related to replication, and uses the WMI Trustmon provider service to verify trust relationships between domains. The WMI Trustmon provider service was introduced in Windows Server 2003 and is not available in earlier versions of Windows. This script raises an event if the WMI Trustmon provider service is not installed. The event provides information on how to install the WMI provider.

You can configure events of varying severity levels to identify critical conditions, error conditions, warning conditions, and informational conditions. You can also set thresholds for the maximum time that can elapse between successful replications and the maximum consecutive number of synchronization failures.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ServerHealth job fails. The default is 35 (magenta event indicator).
Monitor essential services?	
Services	
DNS Client	Select **Yes** to monitor the health of the DNS Client service. The default is Yes.
DNS Server	Select **Yes** to monitor the health of the DNS Server service. The default is Yes.
Event Log	Select **Yes** to monitor the health of the Event Log service. The default is Yes.
File Replication Service	Select **Yes** to monitor the health of the File Replication Service (FRS) service. The default is Yes.
Intersite Messaging	Select **Yes** to monitor the health of the Intersite Messaging service. The default is Yes.
Kerberos Key Distribution Center	Select **Yes** to monitor the health of the Kerberos Key Distribution Center (KDC) service. The default is Yes.
Net Logon	Select **Yes** to monitor the health of the Net Logon service. The default is Yes.
Server	Select **Yes** to monitor the health of the Server service. The default is Yes.

Description	How to Set It
Windows Management Instrumentation (for monitoring)	Select **Yes** to monitor the health of the Windows Management Instrumentation (WMI) service. The default is Yes.
Windows Time	Select **Yes** to monitor the health of the Windows Time service. The default is Yes.
Workstation	Select **Yes** to monitor the health of the Workstation service. The default is Yes.
Event Notification	
Raise event if service is installed but not running?	Select **Yes** to enable events if the monitored service is installed but has not been started. The default is Yes.
Event severity when service not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which the monitored service is installed but has not been started. The default is 10 (red event indicator).
Monitor Active Directory replication?	
Event Notification	
Raise event if WMI replication provider not installed?	Select **Yes** to raise an event if the WMI Active Directory replication provider service is not found. The default is Yes.
Event severity when WMI replication provider not installed	Set the severity level, from 1 to 40, to indicate the importance of an event in which the WMI Active Directory replication provider service is not found. The default is 30 (blue event indicator).
Raise event if replication is not healthy?	Select **Yes** to raise an event if replication error conditions are detected. The default is Yes.
Error threshold -- Maximum time since last successful replication	Specify the maximum number of days that can elapse since the last successful replication occurred. If the threshold is exceeded, an event is raised. The default is 3 days.
Warning threshold -- Maximum consecutive sync failures	Specify the maximum number of synchronization failures that can occur before an event is raised. The default is 3 failures.
Event severity for critical error event	Set the severity level, from 1 to 40, to indicate the importance of an event in which a condition is detected that constitutes a critical error. The default is 5 (red event indicator). An event is always raised if a critical error is detected.
Event severity for Error event	Set the severity level, from 1 to 40, to indicate the importance of an event in which a medium-severity event condition is detected. The default is 10 (red event indicator).
Event severity for Warning event	Set the severity level, from 1 to 40, to indicate the importance of an event in which a high-severity event condition is detected. The default is 20 (yellow event indicator).
Raise event if replication is healthy?	Select **Yes** to raise an event if no replication error conditions are detected. The default is unselected.
Event severity for Information event	Set the severity level, from 1 to 40, to indicate the importance of an event in which a low-severity event condition is detected. The default is 30 (blue event indicator).
Monitor trusts?	
Trust verification level	Select the verification level to use for trust verification: **SC_QUERY**, **Password**, or **SC_RESET**. The default is Password. In order for the parameter setting to take effect, restart the WMI service after you run the job for the first time. **Important** Restarting the WMI service can cause Knowledge Script jobs to fail and raise events. Stop any running Knowledge Script jobs before restarting the WMI service.

Description	How to Set It
Event Notification	
Raise event if WMI Trustmon provider is not installed?	Select **Yes** to raise an event if the WMI Trustmon provider service cannot be found. The default is Yes.
Event severity when WMI Trustmon provider not installed	Set the severity level, from 1 to 40, to indicate the importance of an event in which the WMI Trustmon provider service cannot be found. The default is 30 (blue event indicator).
Raise event if Windows trust in error?	Select **Yes** to raise an event if an error is found in the Windows trust. The default is Yes.
Event severity when Windows trust in error	Set the severity level, from 1 to 40, to indicate the importance of an event in which an error is found in the Windows trust. The default is 10 (red event indicator).
Raise event if trusts are found that cannot be monitored?	Select **Yes** to raise an event if trusts are found that cannot be monitored. **Note** The WMI Trustmon provider (installed by default on Windows Server 2003) can only monitor Windows trusts that are inbound-only. Non-Windows trusts cannot be monitored with this script. The default is unselected.
Event severity when trusts not monitored	Set the severity level, from 1 to 40, to indicate the importance of an event in which trusts are found that cannot be monitored. The default is 25 (blue event indicator).

SyncRequest

Use this Knowledge Script to monitor the number of failed Active Directory replication synchronization requests from the target server. This script raises an event if the number of synchronization requests that fail per second exceeds the threshold you set.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counters
NTDS DirectoryServices	The following counters are used to determine the number of failed sync requests: • DRA Sync Requests Made • DRA Sync Requests Successful

The number of failed sync requests is calculated using the following formula:

```
(DRA Sync Requests Made - DRA Sync Requests Successful)
```

The number of failed sync requests for the current iteration is computed by subtracting the number of failed sync requests at the previous iteration. The percentage of failed synchronization requests since the past iteration is computed and used for threshold comparison.

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SyncRequest job fails. The default is 35 (magenta event indicator).
Monitor synchronization failure rate?	
Event Notification	
Raise event if sync failure rate exceeds threshold?	Select **Yes** to raise an event if the sync failure rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum sync failure rate	Specify the maximum percentage of synchronization requests that can have failed since the last script iteration before an event is raised. The default is 90%.
Event severity when sync failure rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the sync failure rate exceeds the threshold. The default is 20 (yellow event indicator).

Description	How to Set It
Data Collection	
Collect data for synchronization failures?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • The synchronization failure rate • The total number of synchronization requests made • The number of successful synchronization requests The default is unselected.

WriteStat

Use this Knowledge Script to monitor the number of Active Directory write operations per second. This script raises an event if the write rate exceeds the threshold you set.

If you use this script to collect data, you can choose what is included in the data stream and data detail message:

- One data stream that records the total write rate. The data detail message describes the percentage of Active Directory write operations that are being performed by various services, including `DRA`, `KCC`, `LDAP`, `LSA`, `NSPI`, `SAM`, `XDS` (Windows 2000 Server), `NTDSAPI` (Windows Server 2003 and Windows Server 2008), and others.
- One data stream that records the total write rate, but without the detail message breakdown
- Data streams that track the total number of write operations per second and the number of writes per second for various services independently. For example, you get additional independent data streams for the write rate of the `DRA`, `KCC`, `LDAP`, `LSA`, `NSPI`, `SAM`, `XDS` (Windows 2000 Server), and `NTDSAPI` services (Windows Server 2003 and Windows Server 2008).

If you collect data, keep in mind that the more data streams and details you collect, the greater the impact on your database management system and overall performance. For example, if you choose the third data collection option, you may want to adjust your archive policies or increase the frequency at which you check the size of Data tables in the AppManager repository.

This script gathers the following Windows performance counter values for use in data collection and threshold monitoring:

Performance Objects	Counters
NTDS DirectoryServices	For monitoring, only the following counter is used to determine whether the threshold has been crossed and an event should be raised: • DS Directory Writes/sec If data collection is enabled and data collection mode 1 or 3 is specified, values for the following counters are included in the data detail message: • DS % Writes from DRA • DS % Writes from KCC • DS % Writes from LDAP • DS % Writes from LSA • DS % Writes from NSPI • DS % Writes from SAM • DS % Writes from XDS (Windows 2000 Server) • DS % Writes from NTDSAPI (Windows Server 2003 and Windows Server 2008)

Resource Objects

Active Directory domain controller

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the WriteStat job fails. The default is 35 (magenta event indicator).
Raise event if write rate exceeds threshold?	Select **Yes** to raise an event if the number of write operations per second exceeds the threshold you set. The default is Yes.
Event Notification	
Threshold -- Maximum write rate	Specify the maximum number of Active Directory write operations allowed per second before an event is raised. The default is 1 write operation per second.
Event severity when write rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of write operations per second exceeds the threshold. The default is 20 (yellow event indicator).
Data Collection	
Collect data for write rate?	Select **Yes** to collect data for charts and reports. If enabled, specify the data collection mode to use in the *Data collection mode* parameter. The default is unselected.
Data collection mode	Specify the type of data you want to collect. The following entries are valid: • enter **1** for one data stream that records the total write rate. The data detail message describes the percentage of Active Directory write operations that are performed by various services. • enter **2** for one data stream that records the total write rate without any detail message. • enter **3** for all eight data streams. The default is 1 (one data stream and detail message).

AD Knowledge Script Groups

The following Knowledge Script Groups (KSGs) are installed as part of the installation of AppManager for Active Directory. Like other Knowledge Scripts for monitoring Active Directory, they are located on the AD Knowledge Script tab. However, they are also accessible from the **RECOMMENDED** Knowledge Script tab.

Tips for Using Knowledge Script Groups

The AD KSGs contain a recommended subset of Active Directory scripts that represent a "best practices" usage of AppManager for monitoring Active Directory in your organization. These KSGs can be used with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all of the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView. For more information, see the topic titled "About policy-based monitoring" in the AppManager Help.

Generally, each of the KSGs is intended to be used only in the role that is specified as part of the description of the group, with the exception of the AD KSG. Unlike the others, the AD KSG leverages the Knowledge Script job delegation feature included with AppManager for Active Directory 6.2. For more information, see "AD Knowledge Script Job Delegation" on page 88.

Whereas the recommended KSGs are designed to be deployed only on the Domain Controllers listed in the description of each group, the AD KSG executes only on role-holding Domain Controllers. The AD KSG should be used as an alternative to all the others; that is, you should either use the AD KSG or each of the separate KSGs as designated.

KSGs are composed of selected scripts from the regular Knowledge Script tabs. When you modify a script, keep in mind that the script that belongs to a KSG is a different copy of the actual script you access from the **AD** tab. The changes you make are not reflected in the script that is part of the KSG.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group, such as a single domain or an entire forest.

If you modify or remove a script associated with one of these RECOMMENDED KSGs and want to restore it to its original form, you can either reinstall AppManager for Active Directory on the repository computer or check in the desired script from the `qdb\kp\ad\<Knowledge Script Group name>` directory.

AD

Deploy this Knowledge Script Group (KSG) to all domain controllers you want to monitor. This comprehensive KSG has the job delegation feature enabled for Knowledge Scripts that support this feature. If you use this KSG, avoid using the other recommended KSGs that do not employ the job delegation feature. For more information about job delegation, see "AD Knowledge Script Job Delegation" on page 88.

The AD KSG contains the following scripts:

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
Authentications	• Collect data for Kerberos authentications? (enabled) • Collect data for NTLM authentications? (enabled)
BridgeheadChange	• Enable job delegation? (enabled)
ClientSessions	• Collect data for number of client sessions? (enabled) • Threshold -- Maximum number of client sessions (250)
DatabaseSize	• Collect data for database disk space usage? (enabled) Advanced Option (**Advanced** Properties tab): • Collect data every 96 job iterations. Calculate Average.
DCAdvertised	None.
DCHealthMonitor	• Collect data for DC health? (enabled) Advanced Option (**Advanced** Properties tab): • Collect data every 12 job iterations. Calculate Average.
DCInSiteConnectivity	• Enable job delegation? (enabled)
DomainConnectivity	• Enable job delegation? (enabled)
EnumerateSites	• Enable job delegation? (enabled)
EventLog	• Filter -- Source (`NTDS KCC`)
EventLog (NetLogon)	None.
EventLog (W32Time)	None.
FSMOChange	• Enable job delegation? (enabled)
FSMOHealth	• Enable job delegation? (enabled)
FSMOPlacement	• Enable job delegation? (enabled)
GlobalCatalogChange	• Enable job delegation? (enabled)
GlobalCatalogHealth	• Enable job delegation? (enabled) • Collect data for global catalog status? (enabled)
KCCConnections	None.
KCCDisabled	• Enable job delegation? (enabled)
KDCRequests	None.
NumberOfObjects	• Enable job delegation? (enabled) • Object class to check (* for all classes) (*) • Raise event if number of objects exceeds threshold? (enabled) • Collect data for number of objects? (enabled) • Number of objects to return (0 for all objects) (1)

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
NumberOfUsersLocked	• Enable job delegation? (enabled) • Collect data for number of locked user accounts? (enabled)
ReplEventLog	None.
ReplSysVol	None.
ResponseTime	• Collect data for response times? (enabled) Advanced Option (**Advanced** Properties tab): • Collect data every 12 job iterations. Calculate Average.
ServerHealth	None.
SyncRequest	None.

AD (all DCs)

Deploy this Knowledge Script Group (KSG) to all domain controllers you want to monitor. This KSG contains the following scripts:

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
Authentications	• Collect data for Kerberos authentications? (enabled) • Collect data for NTLM authentications? (enabled
ClientSessions	• Collect data for number of client sessions? (enabled) • Threshold -- Maximum number of client sessions (250)
DatabaseSize	• Collect data for database disk space usage? (enabled) Advanced Option (**Advanced** Properties tab): • Collect data every 96 job iterations. Calculate Average.
DCAdvertised	None.
DCHealthMonitor	• Collect data for DC health? (enabled) Advanced Option (**Advanced** Properties tab): • Collect data every 12 job iterations. Calculate Average.
DCInSiteConnectivity	None.
EventLog (NetLogon)	None.
EventLog (W32Time)	None.
EventLog	• Filter -- Source (`NTDS KCC`)
KCCConnections	None.
KDCRequests	None.
ReplEventLog	None.
ReplSysVol	None.
ResponseTime	• Collect data for response times? (enabled) Advanced Option (**Advanced** Properties tab): • Collect data every 12 job iterations. Calculate Average.
ServerHealth	None.
SyncRequest	None.

AD (one DC per domain)

Deploy this Knowledge Script Group (KSG) to a single domain controller per domain. This KSG contains the following scripts:

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
DomainConnectivity	None.
FSMOChange	None.
FSMOHealth	None.
FSMOPlacement	None.
NumberOfObjects	• Object class to check (* for all classes) (*) • Raise event if number of objects exceeds threshold? (enabled) • Collect data for number of objects? (enabled) • Number of objects to return (0 for all objects) (1)
NumberOfUsersLocked	• Collect data for number of locked user accounts? (enabled)

AD (one DC per forest)

Deploy this Knowledge Script Group (KSG)to a single domain controller per forest. This KSG contains the following scripts:

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
BridgeheadChange	None.
EnumerateSites	None.
GlobalCatalogChange	None.

AD (one DC per site)

Deploy this Knowledge Script Group (KSG) to a single domain controller per site. This KSG contains the following scripts:

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
GlobalCatalogHealth	• Collect data for global catalog status? (enabled)
KCCDisabled	None.

Chapter 4
AD-RT Knowledge Scripts

The AD-RT category provides the following Knowledge Scripts for monitoring Active Directory response time.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
CheckDomainController	Checks Active Directory domain controller connectivity.
DNSNameLookup	Checks ability of a DNS server to resolve a particular hostname.
DNSSpecificServerNameLookup	Checks ability of a DNS server to resolve a particular hostname on a specific server.
GetObject	Retrieves content from the Active Directory server.
QueryService	Monitors the availability and status of a service on a computer in the Active Directory domain.
Report_AD-RT	Generates a report on availability and response time.
Report_AD-RT_DNS	Generates a report on DNS availability and response time.

CheckDomainController

Use this Knowledge Script to monitor Active Directory Domain Controllers (DCs). The Knowledge Script checks to see if the DC is running; if it is, the Knowledge Script measures response time information for a performance check.

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Availability**–Returns one of the following values:
  - 1 or 100 – the transaction was successful
  - 0 – the transaction was not successful

  The Availability data point is an indication of whether the test succeeded or failed.
- **Response time**

  The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.

  A Response Time data stream is only generated if the entire transaction is successful.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. For more information, see the description of the **Event on** parameter, below.

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The AD-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is not generated.
- The transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

Enter the name of the Domain Controller as the server when using this Knowledge Script in a service connection.

Resource Objects

Active Directory response time clients (AD-RT)

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	

Description	How to Set It
Collect data for availability?	Select the **Yes** check box to collect data for graphs and reports. If enabled, returns: • 1 or 100 -- Transaction completed successfully • 0 -- Transaction did not complete successfully By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime used a 0 (“not available”) or 1 (“available”) format to indicate availability. You now have the option to use a 0 (“not available”) or 100 (“available”) format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, events are enabled.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5. If you disable availability failure events, this value is ignored.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect response time data for graphs and reports. By default, data is collected.
Threshold -- Maximum response time (seconds)	Specify the maximum number of seconds that the transaction can take before an event is raised. The event message contains a breakdown of the total response time. The default is 5 seconds.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the response time exceeds the threshold. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15.
Domain controller name	Enter the name of the Domain Controller that should receive the response time test flows. If you are setting the **Event on** parameter, the **Domain Controller name** parameter lets you select the server where the event will appear in your console. Enter the name of the server, or click the browse button ([**...**]) to select from a list of available servers. The Domain Controller you select must already be in the TreeView.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent**, the client computer in the response-time tests. This is the default. • **Server,** the Domain Controller being tested • **Both.** The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Logon	
Username	Enter the username to use to log onto the DC.
Password	Enter the password associated with this user.
Domain	Enter the domain name associated with this user.

DNSNameLookup

Use this Knowledge Script to check the ability of your Domain Name System (DNS) server to resolve a particular hostname. If the hostname is not found, the Knowledge Script generates a success event and continues to run to indicate that it was able to contact the DNS server.

Note
The local hosts file will never be used, even if it is enabled on the client.

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Availability**

  This data stream returns one of two values depending on the data stream format you selected:

  - 1 or 100 = transaction was successful
  - 0 = transaction was not successful

- **Response Time**

  The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.

  A Response Time data stream is only generated if the entire transaction is successful.

If this Knowledge Script is able to connect to the specified DNS server, data streams for Availability (showing 100 for available) and response time are created, regardless of whether the hostname you supplied can be resolved or not.

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The AD-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is not generated.
- The job transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

Resource Objects

Active Directory response time clients (AD-RT)

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect data for graphs and reports. If enabled, returns: • 1 or 100 -- Transaction completed successfully • 0 -- Transaction did not complete successfully By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime used a 0 (“not available”) or 1 (“available”) format to indicate availability. You now have the option to use a 0 (“not available”) or 100 (“available”) format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, events are enabled.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5. If you disable availability failure events, this value is ignored.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect response time data for graphs and reports. By default, data is collected.
Threshold -- Maximum response time (seconds)	Specify the maximum number of seconds that the transaction can take before an event is raised. The event message contains a breakdown of the total response time. The default is 5 seconds.
Raise event when threshold is exceeded?	Select the **Yes** check box to raise an event when the response time exceeds the threshold. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15.
Hostname to resolve	Enter the name of the host computer to be resolved.

DNSSpecificServerNameLookup

Use this Knowledge Script to check the ability of your Domain Name System (DNS) server to resolve a particular hostname on a specific server. If the hostname is not found, the Knowledge Script generates a success event and continues to run indicating that it was able to contact the DNS server.

The value you supply for the **Hostname to resolve** parameter must be a fully-qualified hostname, or the transaction will fail with an execution error.

Note
The local hosts file will never be used, even if it is enabled on the client.

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Availability**

  This data stream returns one of two values depending on the data stream format you selected:

  - 1 or 100 = transaction was successful
  - 0 = transaction was not successful

- **Response Time**

  The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.

  A Response Time data stream is only generated if the entire transaction is successful.

If this Knowledge Script is able to connect to the specified DNS server, data streams for Availability (showing 100 for available) and response time are created, regardless of whether the hostname you supplied can be resolved or not.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. For more information, see the description of the **Event on** parameter, below.

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The AD-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is *not* generated.
- The job transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, and the value = 0.

Resource Objects

The Active Directory response time clients (AD-RT)

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect availability data for graphs and reports. By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime used a 0 (“not available”) or 1 (“available”) format to indicate availability. You now have the option to use a 0 (“not available”) or 100 (“available”) format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, events are enabled.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5. If you disable availability failure events, this value is ignored.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect response time data for graphs and reports. By default, data is collected.
Threshold -- Maximum response time (seconds)	Specify the maximum number of seconds that the transaction can take before an event is raised. The event message contains a breakdown of the total response time. The default is 5 seconds.
Raise event when threshold is exceeded?	Select the **Yes** check box to raise an event when the response time exceeds the threshold. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15.
DNS server name	Enter the hostname of the DNS server to query, with no spaces. If you are setting the **Event on** parameter, the **DNS Server name** parameter lets you select the server where the event will appear in your console. Enter the name of the server, or click the browse button ([**...**]) to select from a list of available servers. The server you select must already be in the TreeView.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent**, the client computer in the response-time tests. This is the default. • **Server,** the DNS server being tested • **Both.** The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Hostname to resolve	Enter the fully qualified name of the host computer to be resolved.

GetObject

Use this Knowledge Script to retrieve content from the Active Directory server. Running this Knowledge Script will indicate the response time and availability of this process. The Knowledge Script returns an error if the object path is not found.

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Availability**

  This data stream returns one of two values depending on the data stream format you selected:

  - 1 or 100 = transaction was successful
  - 0 = transaction was not successful

- **Response time**

  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to 3 response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. For more information, see "Setting Parameter Values" on page 220.

  A Response Time data stream is only generated if the entire transaction is successful.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. For more information, see the description of the **Event on** parameter, below.

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The AD-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is not generated.
- The job transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

Resource Objects

Active Directory response time clients (AD-RT)

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	

Description	How to Set It
Collect data for availability?	Select the **Yes** check box to collect data for graphs and reports. If enabled, returns: • 1 or 100 -- Transaction completed successfully • 0 -- Transaction did not complete successfully By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime used a 0 (“not available”) or 1 (“available”) format to indicate availability. You now have the option to use a 0 (“not available”) or 100 (“available”) format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, events are enabled.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5. If you disable availability failure events, this value is ignored.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect response time data for graphs and reports. By default, data is collected.
Threshold -- Maximum response time (seconds)	Specify the maximum number of seconds that the transaction can take before an event is raised. The event message contains a breakdown of the total response time. The default is 5 seconds.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the response time exceeds the threshold. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15.
Response Time Breakdown	
Collect data for binding object?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to bind to the specified object. By default, separate response-time data streams are not collected.
Collect data for listing containers?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to list the containers in which the object is located. This data stream can only be collected if you enabled the **List container objects?** parameter. By default, separate response-time data streams are not collected.
Collect data for downloading objects or containers?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to download any objects or containers from the domain controller. This data stream can only be collected if you enabled the **Download container objects?** parameter. By default, separate response-time data streams are not collected.
Target computer	Enter the hostname of the domain controller, or click the browse button ([**...**]) to select from a list of available servers. The “target computer” is used to enable retrieval of data streams by AppManager Analysis Center v2.0 and higher. If specified, it will also be used in place of “Default Active Directory Server” in the data stream legend. If you are setting the **Event on** parameter, the **Target computer** parameter also determines the computer where the event will appear in your console. The computer you select must already be in the TreeView.

Description	How to Set It

Object path	`ADsPath` of object to be processed. This is in the form:
	`<provider name>://<distinguished name>`
	where:
	• `<provider name>` is the name of the AD Service provider you want to use. Typical ones are LDAP and WinNT. This is case-sensitive.
	• `<distinguished name>` is a provider-specific path and name that uniquely describe the location of the resource.
	For LDAP, a distinguished name might be
	`CN=RALD01,ou=Domain Controllers,dc=netiq,dc=local`
	For WinNT, it might be
	`netiq.local/raldc01/QA`

List container objects?	Select the **Yes** check box to perform the action of listing the resources the object contains. There is a maximum of 1000 objects. You can enable the collection of response time for this action as a separate step.
Download container objects?	Select the **Yes** check box to perform the action of downloading the objects. There is a maximum of 1000 objects. You can enable the collection of response time for this action as a separate step. **Note** If **List container objects** is disabled and **Download container objects** is disabled, *or* if the object is not a container, the system times the action of downloading information about the object itself. **Note** You cannot enable **List container objects** and disable **Download container objects** when the object is a container.
Maximum number of container objects	Enter a value, from 1 to 1000, that specifies the maximum number of objects in the container. The default is 1000.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent**, the client computer in the response-time tests. This is the default. • **Server**, the server being tested • **Both**. The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Logon	
Username	Enter the username to use to log onto the Active Directory server.
Password	Enter the password associated with this user.
Domain	Enter the domain name associated with this user.

QueryService

Use this Knowledge Script to monitor the availability and status of a service on a computer in the Active Directory domain.

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Availability**

  This data stream returns one of two values depending on the data stream format you selected:

  - 1 or 100 = transaction was successful
  - 0 = transaction was not successful

- **Response Time**

  The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.

  A Response Time data stream is only generated if the entire transaction is successful.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. For more information, see the description of the **Event on** parameter, below.

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The AD-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is not generated.
- The job transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

Interactive User

You have the option to run this Knowledge Script as "Interactive User," which requires a user to be physically logged into the computer for the test to run. You might want to do this in environments where a firewall is preventing access to an Active Directory domain controller, or where the test computer is part of a workgroup and not part of a domain. With this feature, the user is not validated, so the test can proceed despite the lack of access to the domain. To run as interactive user, type `Interactive User` for the **Run As Username** parameter, and leave the **Password** and **Domain** parameters blank.

Resource Objects

Active Directory response time clients (AD-RT)

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect data for graphs and reports. If enabled, returns: • 1 or 100 -- Transaction completed successfully • 0 -- Transaction did not complete successfully By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime used a 0 (“not available”) or 1 (“available”) format to indicate availability. You now have the option to use a 0 (“not available”) or 100 (“available”) format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, events are enabled.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5. If you disable availability failure events, this value is ignored.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Threshold -- Maximum response time (seconds)	Specify the maximum number of seconds that the transaction can take before an event is raised. The event message contains a breakdown of the total response time. The default is 5 seconds.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the response time exceeds the threshold. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15.
Host computer	Enter the name of the computer where the service is to be monitored, or click the browse button ([**...**]) to select from a list of available servers. If you are setting the **Event on** parameter, the **Target computer** parameter also determines the computer where the event will appear in your console. The computer you select must already be in the TreeView.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent**, the client computer in the response-time tests. This is the default. • **Server,** the server being tested • **Both**. The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Service	

Description	How to Set It
Service name	Enter the internal name of the service to query, with no spaces. To find the service name in Windows 2000 or later, open the Control Panel and select **Administrative Tools > Services**. Right-click a service name and select **Properties** in the pop-up window. The **Service name** field appears at the top of the Properties dialog box.
Verify if service is running?	Select the **Yes** check box to query the state of the specified service name and verify whether it is running. By default, the service state is not verified.
Raise event if service is not running?	Select the **Yes** check box to raise an event if the service is not running. By default, events are not raised.
Event severity when service is not running	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 20. If you disable service events, this value is ignored.
Logon and Run As	
Username	Enter the domain username of a user who has Administrator privileges on the host computer. Interactive User is also a possible value. Leave the Password and Domain parameters blank if you specify “Interactive User”.
Password	Enter the password associated with this user. Leave blank to run as “Interactive User.”
Domain	Enter the domain name associated with this user. Leave blank to run as “Interactive User.”
Administrators group on managed client	Enter the name of the Administrators Group on the managed client. Typically, this name is “Administrators”. The default is “`Administrators`”.

Report_AD-RT

Use this Report Knowledge Script to generate a report detailing availability and response time for the following AD-RT Knowledge Scripts:

- CheckDomainController
- GetObject
- QueryService

Resource Object

AppManager repository

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	Use the following parameters to select the data for your report.
KS for report	Select the Knowledge Script on which to report: 1. Click the **...** button to show the Filter KS List dialog box. 2. Select a filter to narrow the list of Knowledge Scripts and click **OK** to display the list of Knowledge Scripts that met the filter specifications. 3. If you click **Cancel** from the Filter dialog box, all the Knowledge Scripts are displayed. 4. Highlight an AD-RT Knowledge Script from the **Knowledge Script Name** list and click **Finish**.
AD-RT client(s)	Select the AppManager ResponseTime for Active Directory client(s). Click the **Browse [...]** button to show the Select View(s) and a filter dialog box. From the **View(s)** list, select from one to 25 views. Your subsequent selections are limited to computers or server groups that are visible in the selected views. Select one of the Filters options: • **View:** Includes all computers in the views you selected. • **Computer:** Select from individual computers in the views you selected. • **Server Group:** Select from server groups in the views you selected. **Note** Selecting a server group includes all computers in that group.
AD Server or “All”	Type the name of the Active Directory server, or type “`All`” to designate all computers as Active Directory servers. The default is the default Active Directory server.
Select time range	In the Select Date/Time Range dialog box, set specific start and end report information dates, which are good for historical or ad hoc reports, or a sliding range that sets the time range of data to include in the report. The sliding range option is useful for reports running on a regular schedule. It is the default.

Description	How to Set It
Select peak weekday(s)	In the Select Peak Weekday(s) dialog box, while selecting, press **Shift** to select a contiguous day range, or press **Ctrl** to select non-contiguous days.
Aggregation by	Select the time unit by which to aggregate data. The default is Hour. This works in conjunction with the next field, **Aggregation interval**, which determines the number of units for one interval of data aggregation.
Aggregation interval	Select the interval units in which to aggregate data. The default is 1. For example, if you aggregate by the Hour and select 1 here, data is aggregated once every hour.
Report Settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter card?	Select the **Yes** check box to display a table of parameters in the report. By default, the table is displayed.
Include Availability Detail table?	Select the **Yes** check box to display the Availability Detail table as part of the report. By default, the table is included.
Include Availability chart?	Select the **Yes** check box to display the Availability chart as part of the report. By default, the chart is included.
Availability data stream format	Specify the data stream format. Options are 0-100 or 0-1. The default format is 0-100.
Threshold on Availability chart	Enter an integer for the percent. The default is 0 (no threshold is displayed).
Include Response Time Detail table?	Select the **Yes** check box to display the Response Time Detail table as part of the report. By default, the table is included.
Include Response Time chart?	Select the **Yes** check box to display the Response Time chart as part of the report. By default, the chart is included.
Units for Response Time report	Select the response time unit of msec (the default) or sec.
Threshold on Response Time chart (selected units)	Enter the units in seconds > 0, or use the default of 0. Zero suppresses the threshold indicator in the chart.
Select chart style	Options in the Chart Settings dialog box set the appearance of the chart. The same parameters are used in both the availability and response time charts, if both are produced. The default is Ribbon.
Select output folder	Select the **...** button to display the Publishing Options dialog box. From this dialog, specify the report filename and the report folder. You can specify a specific folder or have the system generate the folder each time the report runs.
Add job ID to output folder name?	Select the **Yes** check box to add a job ID to the output folder name. By default, the job ID is not added.
Index-Report Title	Select the **...** button to display the Report Properties dialog box. From this dialog, you can configure report title settings and custom fields.
Add timestamp to title?	Specify whether to add a timestamp to the report title.
Event Notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Generate event on success?	Select the **Yes** check box to raise an event when a report is generated. By default, events are raised.
Severity level for report success	Set the severity level for a successful report. The default is 35.
Severity level for report with no data	Set the severity level for a report with no data. The default is 25.
Severity level for report failure	Set the severity level for a report with no data. The default is 5.

Report_AD-RT_DNS

Use this Report Knowledge Script to generate a report detailing availability and response time for the following AD-RT DNS Knowledge Scripts:

- DNSNameLookup
- DNSSpecificServerNameLookup

Resource Object

AppManager repository

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	Use the following parameters to select the data for your report.
KS for report	Select the Knowledge Script on which to report: 1. Click the **...** button to show the Filter KS List dialog box. 2. Select a filter to narrow the list of Knowledge Scripts and click **OK** to display the list of Knowledge Scripts that met the filter specifications. 3. If you click **Cancel** from the Filter dialog box, all the Knowledge Scripts are displayed. 4. Highlight a AD-RT Knowledge Script from the **Knowledge Script Name** list and click **Finish**.
AD-RT client(s)	Select the AppManager ResponseTime for Active Directory client(s). Click the **Browse [...]** button to show the Select View(s) and a filter dialog box. From the **View(s)** list, select from one to 25 views. Your subsequent selections are limited to computers or server groups that are visible in the selected views. Select one of the Filters options: • **View:** Includes all computers in the views you selected. • **Computer:** Select from individual computers in the views you selected. • **Server Group:** Select from server groups in the views you selected. **Note** Selecting a server group includes all computers in that group.
AD Server or “All”	Type the name of the DNS server, or type “`All`” to designate all computers as DNS servers. The default is the default DNS server.
Select time range	In the Select Date/Time Range dialog box, set specific start and end report information dates, which are good for historical or ad hoc reports, or a sliding range that sets the time range of data to include in the report. The sliding range option is useful for reports running on a regular schedule. It is the default.
Select peak weekday(s)	In the Select Peak Weekday(s) dialog box, press **Shift** to select a contiguous day range, or **Ctrl** to select non-contiguous days.

Description	How to Set It
Aggregation by	Select the time unit by which to aggregate data. The default is Hour. This works in conjunction with the next parameter **Aggregation interval**, which determines the number of units for one interval of data aggregation.
Aggregation interval	Select the interval units in which to aggregate data. The default is 1. For example, if you aggregate by the Hour and select 1 here, data is aggregated once every hour.
Report Settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter card?	Select the **Yes** check box to display a table of parameters in the report. By default, the table is included.
Include Availability Detail table?	Select the **Yes** check box to display the Availability Detail table as part of the report. By default, the table is included.
Include Availability chart?	Select the **Yes** check box to display the Availability chart as part of the report. By default, the chart is included.
Availability data stream format	Specify the data stream format. Options are 0-100 or 0-1. The default format is 0-100.
Threshold on Availability chart	Enter an integer for the percent. The default is 0 (no threshold is displayed).
Include Response Time Detail table?	Select the **Yes** check box to display the Response Time Detail table as part of the report. By default, the table is included.
Include Response Time chart?	Select the **Yes** check box to display the Response Time chart as part of the report. By default, the chart is included.
Units for Response Time report	Select the response time unit of msec (the default) or sec.
Threshold on Response Time chart (selected units)	Enter the units in seconds > 0, or use the default of 0 (no threshold indicator on the chart).
Select chart style	Options in the Chart Settings dialog box set the appearance of the chart. The same parameters are used in both the availability and response time charts, if both are produced. The default is Ribbon.
Select output folder	Select the **...** button to display the Publishing Options dialog box. From this dialog, specify the report filename and the report folder. You can specify a specific folder or have the system generate the folder each time the report runs.
Add job ID to output folder name?	Select the **Yes** check box to add a job ID to the output folder name. By default, the job ID is not added.
Index-Report Title	In the Report Properties dialog box, configure report title settings.
Add timestamp to title?	Select the **Yes** check box to add a timestamp to the report title.
Event Notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Generate event on success?	Select the **Yes** check box to raise an event when a report is generated. By default, events are raised.
Severity level for report success	Set the severity level for a successful report. The default is 35.
Severity level for report with no data	Set the severity level for a report with no data. The default is 25.
Severity level for report failure	Set the severity level for a report with no data. The default is 5.

Chapter 5
AMAdmin Knowledge Scripts

The AMAdmin category contains Knowledge Scripts that perform administrative tasks for Windows agents and your AppManager site. To run Knowledge Scripts in this category, your user account needs administrator privileges.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AgentConfigMSRestrictions	Configures the agent restrictions for communicating with management servers.
AgentConfigSecurityKey	Updates the security key file on a managed client computer.
AgentConfigSecurityLevel	Configures the security level for the AppManager agent remotely on Windows computers in your network.
AgentHealth	Monitors the Windows Application log for self-monitoring events raised by the agent services (`NetIQmc` and `NetIQccm`).
AgentSelfMon	Monitors the health of the scripting engine on the AppManager agent on a Windows computer.
ChangeFooter	Changes the graphic and hyperlink that appear at the bottom of each report page.
ConcurrentRpt	Queries the registry on a computer where you have installed a report agent to get or set the number of concurrent reports.
ConfigAdminEvents	Updates the registry with severity settings for AppManager agent and Management Service events
ConfigSiteCommType	Configures communication between managed client computers and the management server.
ConfigSiteNetFlowCtrl	Configures the size and frequency of agent communications with the management server.
DBHealth	Monitors SQL Server resources associated with the AppManager repository.
DeleteExpiredReports	Deletes expired reports generated by an AppManager report agent.
DisableSiteComm	Temporarily disables network communication from a managed client on Windows to the current management server and saves messages (including events, data, and job status) in the managed client's local repository.
EnableSiteComm	Resumes regular ongoing network communication from a managed client on Windows to the management server.
GreyMachines	Monitors AppManager agents that do not respond to management server Ping requests.

Knowledge Script	What It Does
IISContinueSite	Continues a paused Internet Information Services (IIS) site.
IISPauseSite	Pauses an Internet Information Services (IIS) site.
IISRestartServer	Restarts an Internet Information Services (IIS) server.
IISRestartSite	Restarts an Internet Information Services (IIS) site.
LRReadParameters	Raises an event that displays local repository (LR) configuration information of a managed client computer.
LRRemoveParameters	Removes local repository (LR) configuration information from a managed client computer.
LRWriteParameters	Stores local repository (LR) configuration information in a managed client computer.
MonitorMSCommunications	Monitors the Windows Application log for events that indicate the agent and the management server are not using compatible encryption keys.
MSHealth	Monitors the Windows Application log for events generated by the agent service and the management server.
RemovePrimaryMS	Removes a designated primary management server from a managed client on Windows.
SchedMaint	Sets an application server maintenance period for a managed computer on Windows. During the maintenance period, regularly scheduled AppManager jobs can be prevented from running.
SetAllowMS	Restricts the management servers that can control a particular agent in sites with multiple management servers or multiple repositories.
SetDataTimeStamp	Sets the timestamp for data as it is referenced for reports. This setting affects all reports, but it does not affect areas other than reporting.
SetDeploymentWebService	Sets or changes the deployment Web service with which the managed client communicates to install the agents remotely.
SetKSStandby	Designates a selected managed client as a standby managed client for specified Knowledge Script categories and for the master managed client.
SetLocalRPSize	Modifies the maximum number of events or data points that can be stored in the local repository of a managed client on Windows.
SetPrimaryMS	Sets the primary management server for a managed client on Windows in multiple management server configurations.
SetReportPaths	Sets the output path of the Report Agent. Sets the URL Mapping registry value so that the paths to reports are displayed as hyperlinks in report event messages.
SetResDependency	Defines the resources required to run Knowledge Script jobs on Windows computers.
SiteSchedUpload	Specifies a schedule for uploading data and/or events from the local repository of a managed client on Windows to the current management server. Sets up specific schedules for data, events, or both.
UpgradeJobs	Upgrades all child jobs for a specified parent job on managed Windows or UNIX servers to the latest Knowledge Script version.

AgentConfigMSRestrictions

Use this Knowledge Script to check for and configure agent restrictions for communicating with management servers. By default, this script raises an event if an agent is configured to allow communication with anonymous management servers.

You should restrict the management servers from which an AppManager agent will accept job requests to ensure that only authorized management servers communicate with the agent.

An *anonymous* management server is a management server with which the agent has not explicitly authorized communication.

The list of management servers with which the agent communicates is stored in the following registry key:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\4.0\NetIQMC\Security\AllowMS
```

If the value of this key is * (asterisk), the agent allows anonymous communication.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

About Authorizing Management Servers

When you upgrade the agent to AppManager 7.x, the upgrade process allows you to automatically restrict the authorized servers to the designated primary and secondary, or keep the current configuration until you change the agent's designated primary and secondary management server using the SetPrimaryMS script. If you do not change the management server designation during the upgrade, you can use this script after you upgrade to restrict the authorized management servers.

AppManager 6.0 (or later) agents by default are configured to authorize communication with their designated primary and secondary management servers. If you did not designate the primary and secondary management server during installation, you can use this script after installation to restrict the authorized management servers.

Authorizing Management Servers in a Single-Site Configuration

If you are managing a client computer from a single AppManager site (repository), you should restrict the authorized management servers to the agent's designated primary and secondary management server.

Authorizing Management Servers in a Multiple-Site Configuration

Within a site, after you designate an agent's primary and secondary management server, the agent receives job information and sends events and data only to its designated primary or secondary management server. However, if you have more than one AppManager site, you may want to allow the agent to accept job requests from another site. To do so, you can use this script to authorize the management servers from each site.

When allowing the agent to accept communication from additional management servers, make sure you choose the **Append** option to **add** the management servers to the authorized list (instead of replacing the existing list of authorized management servers). This will allow you to run the SetPrimaryMS script on the agent from the other site and properly configure the agent to accept communication from management servers in both sites.

Reading the Current Configuration

If you have AppManager 5.0.1 agents, or if you are unsure of the agent settings, view the current configuration by choosing **Read configuration** from the *Select operation* parameter and selecting an option to raise an event:

- **If an insecure configuration is detected** – The event message indicates the agent's configuration allows anonymous management server communication. If you choose this option, you can also set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
- **To report current configuration** – The event message indicates the agent configuration. If you choose this option, you can also set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

When reading the current configuration, by default this script raises an event of severity level 10 if an insecure configuration is detected.

This script always raises an event if the job fails.

This script raises an event for each agent to report the agent's configuration. To view the results, click the **Message** tab.

The event message contains the following sections:

- **Current configuration** – Indicates whether the agent is Select allow anonymous communication (that is, communication with management servers with which the agent has not explicitly authorized communication).

Result	What It Means
Never allow anonymous MS	The agent is configured to restrict anonymous management server communication. You must run this script to allow anonymous management server communication. This result only applies to version 6.0 (or later) agents. If you configured a version 5.0.1 (or earlier) agent to never allow anonymous management servers, the configuration is *Do not allow anonymous MS at this time* until you upgrade the agent.
Do not allow anonymous MS at this time	The agent is configured to restrict anonymous communication. For 5.0.1 agents, this result means that when you upgrade the agent, you can change the agent configuration to allow anonymous communication.
Allow anonymous MS until Primary/Secondary MS is set	The agent is configured to allow anonymous communication until you designate a primary management server. If the agent that has not been configured to have a designated primary server, select this option to secure management server communication after the primary management server is designated.
Allow anonymous MS at this time	The agent is configured to remove restrictions on anonymous management server communication. This setting is not recommended.

- **Specified management servers currently allowed to communicate with this agent** – Lists the management servers that are authorized to communicate with the agent.

If this section lists the value as **[Blank]**, the agent does not have an authorized list of management servers with which to communicate. In this case, the agent can still communicate with its designated primary and secondary management server. We recommend that you authorize the agent to communicate with its primary and secondary management server.

Changing the Current Configuration

To change the current configuration, choose **Write configuration** from the *Select operation* parameter and specify the following parameters. By default, this script reads the configuration.

This script always raises an event if the job fails.

Set or change the following parameters as needed:

Parameter	How to Set It
Write Options	
Restrict management server communication	Select an option to restrict management server communication: • **Never allow anonymous MS** -- For AppManager 6.0 (or later) agents, this option restricts anonymous management server communication. For AppManager 5.0.1 (and earlier) agents, this option restricts anonymous communication and, when you upgrade the agent, prevents you from changing the agent configuration to allow anonymous communication. If you configured a 5.0.1 (or earlier) agent with this option, the agent is configured to **Do not allow anonymous MS at this time** until you upgrade the agent. **Tip** To configure an agent to allow anonymous communication, run this script and select the **Allow anonymous MS at this time** option. If you choose this option, make sure the agent is configured to authorize communication with at least one management server. This is the default. • **Do not allow anonymous MS at this time** -- This option restricts anonymous communication for all versions of the agent. For 5.0.1 (or earlier) agents, this option allows you to change the agent configuration after you upgrade to allow anonymous communication. • **Allow anonymous MS until Primary/Secondary MS is set** -- This restricts anonymous management server communication after the primary management server is designated. If the agent that has not been configured to have a designated primary server, select this option to allow anonymous communication until you designate a primary management server. • **Allow anonymous MS at this time** -- This option removes restrictions on anonymous management server communication. This setting is not recommended.

Parameter	How to Set It
List of authorized management servers	Specify the management servers you want to authorize: • **Management servers to include** -- Specify a comma-separated list of the management servers with which you want the agent to communicate. • **Append or replace current list?** -- Select one of the following options: **Append** to add your specified management servers to the list of authorized management servers. This is the default. **Replace** to remove the existing list of authorized management servers and replace with your specified management servers. • **Management servers to remove** -- Specify a comma-separated list of the management servers with which you do **not** want the agent to communicate.
Event notification	Set this script to raise an event and specify the severity if: • **Configuration succeeds --** Select the **Yes** check box to raise an event if the configuration succeeds. When enabled, lets you also set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 20 (yellow event indicator). By default, this option is enabled. • **Configuration failed** -- Select the **Yes** check box to raise an event if the configuration fails. When enabled, lets you also set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10 (red event indicator). By default, this option is enabled.

Avoiding Orphaned Agents

If you use this script to remove or replace the list of authorized management servers and the agent is configured to never allow anonymous management server communication, make sure you authorize at least one valid management server. If the agent is configured to never allow anonymous management server communication and the agent is not configured to authorize a management server, the agent cannot be managed by AppManager.

To resolve this problem, manually edit the registry on the managed client computer to specify an authorized management server list in `\HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\4.0\NetIQMC\Security\AllowMS`.

AgentConfigSecurityKey

Use this Knowledge Script to remotely update the security key information on your managed Windows computers in an AppManager site if you are using encrypted communication or authentication and encryption to secure communication between management servers and managed clients.

Within an AppManager site, all management server computers and managed Windows clients must use the same security key information. This key information is stored in the repository and extracted from the repository into an encrypted and password-protected agent key file. You can then use this script to distribute this password-protected key file to remote agents. If the AppManager repository has different key information than an AppManager agent, agent will not be able to decrypt information from the management server and communication will fail.

Note
Use this script only to distribute the key file to managed Windows clients. You must create the key information and the agent key file separately before using this script. In most cases, you create key information when you install the AppManager repository or manually using the NQKeyGenWindows utility. If your environment includes older AppManager agents (versions 5.0.1 or 6.0), you should update those agents before attempting to distribute a new key file. If you have an existing key file generated by the NetIQ Encryption utility (rpckey.exe) in a previous release, you can continue to use that key file and distribute it to AppManager 7.x agents, if needed, until you are ready to replace the old key file with one generated with the NQKeyGenWindows utility.

After you distribute an updated key file to all of the Windows agents, including the agent on the management server computers within your site in your site, you will experience a temporary loss of communication between the management server and the agents. To have the management server receive the new security key information from the repository database and resume communication with the updated Windows agents, you must stop and restart the NetIQ AppManager Management Service (`NetIQms`).

Note
If you already distributed an AppManager 7.x key file to your Windows agents, you can use the same key file for both Encrypted and Encrypted and Authenticated communication. You do not need to re-key your Windows agents to change the security level for those agents.

For more information, see "Using Secure Communication for Windows Agents" and "Key File Utility for Windows Agents" in the *Administrator Guide for AppManager*. For more information about configuring security after an AppManager upgrade, see the *Upgrade and Migration Guide for AppManager*.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Location of key file	Provide the full path to the agent key file. For example: `C:\temp\nqWindowsPublic0.key` To specify some other computer in the environment rather than the target computer, type the UNC path to the file. For example, if the key is stored in the `E:\Temp` folder on the computer `zebra`: `\\zebra\e$\temp\nqWindowsPublic0.key`
Encryption password	Provide the password you specified when you created the agent key file. The characters that you type appear as asterisks to protect your password.
Raise event if the update succeeds?	Select **y** to raise an event when the key is successfully updated on the target computer. The default is y.
Event severity when the update succeeds	Set the event severity level, from 1 to 40, to indicate the importance of a successful registration of the management server. The default severity level is 25 (blue event indicator).

AgentConfigSecurityLevel

Use this Knowledge Script to remotely update the agent security level on the managed Windows computers in your site. When configuring the security level for the agent, keep in mind that all managed Windows clients and management server computers in an AppManager site must be configured to use the same security level. For more information about implementing AppManager secure communication, see the *Administrator Guide for AppManager*.

Use this script to change the security level on the managed Windows clients in your AppManager site either before or after you change the security level on the repository database. The new security level takes effect on the agent as soon as the script completes.

If your repository database is configured to use Encryption or Encryption and Authentication, and you change the security level on the agent to Cleartext, this script will not immediately raise a successful event. In this case, the agent cannot communicate with the management server until you change the security level on the repository database and restart the management server.

The following security levels are available:

- **0 - Cleartext ~ no security** indicates that all communication between the agent and the management server is in cleartext and is not encrypted. This option is available for all supported versions of the AppManager agent.
- **1 - Encryption ~ medium security** indicates that all communication between the agent and the management server is encrypted but the agent does not authenticate the identity of the management server. This option is available for all supported versions of the AppManager agent.
- **2 - Encryption and authentication ~ highest security** indicates that the agent will attempt to authenticate the identity of the management server before sending and receiving encrypted communication. This option is available for version 6.0 (or later) of the AppManager agent.

To use the AgentConfigSecurityLevel script to increase the security level on your Windows agents (for example, from Cleartext to Encryption and Authentication):

1. Use the `NQKeyGenWindows.exe` utility to generate an encryption key file and insert it into the repository database. You can find this utility in the `Program Files\NetIQ\AppManager\bin` directory.

   Note
   The same key file can be used for both encrypted and encrypted and authenticated communication.

2. If you have not done so already, use the AgentConfigSecurityKey script to distribute the agent portion of the key file to all of your Windows agents, including the agent on the management server computers within your site.
3. Use the `NQKeyGenWindows.exe` utility to change the security level on the repository database.
4. Use the AgentConfigSecurityLevel script to change the security level on the agents, including the agent on the management server computers within your site.
5. Stop and restart the NetIQ AppManager management server service (`NetIQms`) to communicate at the specified security level.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Security level	Select the security level you want the managed Windows computer to use: • **0 - Clear text** if you want all communication between the agent and the management server to be in clear text and is not encrypted. This option is best for closed network environments, testing, or troubleshooting communication issues. • **1 - Encryption** if you want all communication between the agent and the management server to be encrypted but do not require authentication. • **2 - Encryption and authentication** if you want the management server to be authenticated before sending and receiving encrypted communication. Keep in mind that, for a single repository, all managed Windows clients must use the same security level setting. Any time you update security, you must do so for all of your Windows agents. If you cannot update all of your WIndows agents at once, the management server will not be able to communicate with those agents and the interruption in communication may result in missing critical events or data. Therefore, you should plan any change to the security level carefully to minimize the chance of communication failures. The default is 0 - Clear text.
Raise event when update succeeds?	Select **y** to raise an event when the security level is successfully updated. This script always raises an event if the job does not run successfully. If enabled, you can configure the severity level of the event. The default is y.
Event severity when the update...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **... succeeds**. If you set this script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **... fails**. The default is 5 (red event indicator).

AgentHealth

Use this Knowledge Script to monitor the status of the AppManager agent, specifically, the Managed Client (MC) and Client Communication Manager (CCM) services. This script looks for self-monitoring events of several types (general, communication, job, security, and upgrade) in the Windows Application log. An event is raised when AppManager places a self-monitoring event in the Windows Application log.

You can filter the event log entries associated with the agent services by specifying a combination of include and exclude strings for each event field. All event log entries that match the filtering criteria are returned in the event detail message.

This script should be run on computers that do not have the Management Server installed. To monitor for self-monitoring events on Management Server computers, use the MSHealth script.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Asynchronous**.

Regardless of the schedule you select, once you start the script, its job status appears as **Running**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Monitor events of type...	Select **y** to raise an event when AppManager places a self-monitoring event in the Windows Application Log of any of the following types: • **... general**. The default is y. • **... communications**. The default is y. • **... job**. The default is y. • **... security**. The default is y. • **... upgrade**. The default is y.
Event severity for events of type...	Set the event severity level, from 1 to 40, to reflect the importance when the following types of event are inserted in the Windows event log: • **... general**. The default is 15 (yellow event indicator). • **... communications**. The default is 15 (yellow event indicator). • **... job**. The default is 15 (yellow event indicator). • **... security**. The default is 15 (yellow event indicator). • **... upgrade**. The default is 15 (yellow event indicator).

Parameter	How to Set It
Filter events by event description	If you set a filter here, the script looks for matching entries in the event log's **Description** field. Multiple strings can be entered, separated by commas. The filter string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary. For example: communication,cold start:mc,ccm
Use case-sensitive description filter?	Select **y** to make all filter statements for this script case-sensitive. The default value is n (not case-sensitive).

AgentSelfMon

Use this Knowledge Script to monitor the health of the scripting engine in the AppManager agent on a Windows computer. In some cases, the scripting engine does not run jobs properly but the AppManager agent may respond to remote procedure calls from AppManager diagnostic utilities. In this case, restarting the AppManager agent and the scripting engine resolves the problem. This script is not applicable on UNIX computers.

This script monitors the health of the scripting engine on the agent by running a job that updates a timestamp value in the Windows registry. If the age of the timestamp value exceeds the threshold you specify, the Client Communication Manager service (`netiqccm.exe`) automatically restarts the AppManager agent service (`netiqmc.exe`).

During the first monitoring interval, the Client Communication Manager service (`netiqccm.exe`) writes the current timestamp value to the Windows registry; subsequent job iterations compare and then update the timestamp value.

The timestamp and threshold values are stored in the registry under `HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0` as follows:

Registry Entry	Registry Location
Timestamp value that is written each time the job runs	NetIQmc\Admin\LastMCCheck
Threshold, in seconds, for the maximum age of timestamp value	NetIQccm\Admin\MCFreezeThreshold

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Every 5 minutes**.

The interval you select must be less than or equal to the value you specify in the *Threshold - Maximum age of timestamp value* parameter.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Threshold --Maximum age of timestamp value	Specify a threshold, in seconds, for the maximum age of the timestamp value. If the elapsed time exceeds the threshold, the Client Communication Manager service (`netiqccm.exe`) automatically restarts the managed client (`netiqmc.exe`). If you specify 0, the current value of the `MCFreezeThreshold` registry key is used. This feature allows you to configure the threshold value a single time. If a value of 0 is specified, the job will not run if the value of `MCFreezeThreshold` is less than the job's scheduled interval. The default value is 0. **Note** If you specify a threshold other than 0, the threshold must be greater than or equal to the scheduled job interval. If the threshold is less than the interval, the job does not run and an event (severity level 40) is raised.

ChangeFooter

Use this Knowledge Script to change the graphic and hyperlink that appear at the bottom of each report page.

The NetIQ logo is the default graphic and the default hyperlink is to the NetIQ Web site. This script allows you to substitute a different graphic and hyperlink, or to restore those settings to the defaults.

Resource Object

AppManager repository object under the Report agent

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if set or restore operation succeeds?	Select **y** to raise an events if the script job succeeds in setting a new report footer or in restoring the default report footer. By default, events are raised.
Set new footer or restore default footer	• Select **Set a new footer** to change the default settings. This option clears the existing values for the *Full path to new picture file*, *Hyperlink text*, and *URL* parameters. • Select **Restore to NetIQ default footer** to restore the default settings. This option restores the default values for the *Full path to new picture file*, *Hyperlink text*, and *URL* parameters.)
Full path to logo image file	Provide the full path to the new picture file you want to use. For example, `C:\LogoFiles\Logo1.gif`.
Hyperlink text	Provide the new text for the hyperlink that appears next to the picture file.
URL for hyperlink	Provide the URL referenced by the hyperlink.
Use actual image size?	Select y to use the actual size of the new footer image. If this parameter is disabled, the image is scaled to the size of the default footer image. The default is y.
Event severity when set or restore operation succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

ConcurrentRpt

Use this Knowledge Script to get the setting for the number of concurrent report jobs that can be managed by a report agent, or to reset that registry key to another value. This script queries the registry on a computer where you have installed a report agent to get or set the number of concurrent reports.

Resource Object

AppManager repository object under the Report agent

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if query or set operation succeeds?	Select **y** to raise events. The default is y. When you query the registry to get the value for the number of concurrent reports, the event detail message contains the current setting.
Query, or set new value?	Set the value to **query** to query the registry and get the value of the registry key. Set the value to **set** to change the value of the registry key. In order for the value to take effect, you must restart the managed client. If you select **set**, use the *Number of concurrent reports* parameter to define the number of concurrent jobs.
Number of concurrent reports (optional)	Define the number of concurrent report jobs managed by the report agent. The default is 3. **Note** Setting this value too high can overload the report agent, slow the generation of reports, and adversely affect the performance of the report agent computer.
Event severity when query or set operation succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

ConfigAdminEvents

Use this Knowledge Script to update event severity settings in the registry: `HKEY_LOCAL_MACHINE\Software\NetIQ\AppManager\4.0`. By using this script, you do not have to manually update severity settings in the registry for the following AppManager agent (`NetIQmc` and `NetIQccm`) and Management Service (`NetIQms`) events:

- Management Service events
  - `NetIQms` administrative alerts updated in the `\netiqms\admin\AdminEvtSev` registry key
  - `NetIQmc` job failures updated in the `netiqms\config\MC Job Abort Event Sev` registry key
  - Orphaned job events updated in the `\netiqms\config\Orphan Job Event Sev` registry key
  - General success events updated in the `\netiqms\admin\General Success Events` registry key
  - General failure events updated in the `\netiqms\admin\General Failure Events` registry key
- AppManager agent events
  - `NetIQmc` administrative alerts updated in the `\netiqmc\admin\AdminEvtSev` registry key
  - Knowledge Script failure events updated in the `\netiqmc\admin\Knowledge Script Failure Events` registry key
  - `NetIQccm` administrative alerts updated in the `\netiqmc\admin\AdminEvtSev` registry key

This script raises events if Management Service and agent event severity settings are applied to the registry, and if the Management Service is not installed on the agent computer.

Notes

- For AppManager versions earlier than 8.x, you must restart the `NetIQmc`, `NetIQms`, and `NetIQccm` services after using this Knowledge Script to update the registry. The updated registry settings do not take effect until you restart the services.
- For more information about AppManager registry settings, see the *Administrator Guide for AppManager*, available on the NetIQ AppManager Documentation Web site.

Prerequisite

AppManager version 8.x is required to support registry updates for the following events. The registry keys for these events are not created in earlier versions of AppManager.

- General success events
- General failure events
- Knowledge Script failure events

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ConfigAdminEvents job fails. The default is 5.
Apply Management Service severity settings to registry?	Select **Yes** to update the registry with severity settings for the following Management Service events: • Administrative alerts • `NetIQmc` job failures • Orphaned job events • General success events • General failure events The default is Yes.
Event severity when administrative alerts applied to registry	Set the severity level, from 1 to 40, to indicate the importance of an event in which severity settings for administrative alerts are applied to the registry. The default is 40.
Event severity when NetIQmc job failures applied to registry	Set the severity level, from 1 to 40, to indicate the importance of an event in which severity settings for NetIQmc job failures are applied to the registry. The default is 10.
Event severity when orphaned job events applied to registry	Set the severity level, from 1 to 40, to indicate the importance of an event in which severity settings for orphaned job events are applied to the registry. The default is 5.
Event severity when general success events applied to registry	Set the severity level, from 1 to 40, to indicate the importance of an event in which severity settings for general success events are applied to the registry. The default is 35. **Note** This parameter is not supported for versions of AppManager earlier than version 8.x.
Event severity when general failure events applied to registry	Set the severity level, from 1 to 40, to indicate the importance of an event in which severity settings for general failure events are applied to the registry. The default is 5. **Note** This parameter is not supported for versions of AppManager earlier than version 8.x.
Apply agent severity settings to registry?	Select **Yes** to update the registry with severity settings for the following agent events: • NetIQmc administrative alerts • Knowledge Script failures • NetIQccm administrative alerts The default is Yes.
Management Client (NetIQmc)	
Event severity when administrative alerts applied to registry	Set the severity level, from 1 to 40, to indicate the importance of an event in which severity settings for NetIQmc administrative alerts are applied to the registry. The default is 40.
Event severity when Knowledge Script failures applied to registry	Set the severity level, from 1 to 40, to indicate the importance of an event in which severity settings for Knowledge Script failures are applied to the registry. The default is 5. **Note** This parameter is not supported for versions of AppManager earlier than version 8.x.

Parameter	How to Set It
Suppress events with severity equal to	Use this parameter to ignore NetIQmc events with a severity equal to the value you provide. The default is a severity level of 0.
Client Communication Manager (NetIQccm)	
Event severity when administrative alerts applied to registry	Set the severity level, from 1 to 40, to indicate the importance of an event in which severity settings for NetIQccm administrative alerts are applied to the registry.The default is 40.
Event Notification	
Raise event if Management Service severity settings successfully applied to registry?	Select **Yes** to raise an event if Management Service severity settings are applied to the registry successfully. The default is Yes.
Event severity when settings successfully applied to registry	Set the severity level, from 1 to 40, to indicate the importance of an event in which Management Service severity settings are applied to the registry successfully. The default is 16.
Raise event if Management Service not installed on agent computer?	Select **Yes** to raise an event if the Management Service is not installed on the agent computer on which you run this script. The default is Yes.
Event severity when Management service not installed on agent computer	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Management Service is not installed on the agent computer on which you run this script. The default is 25.
Raise event if agent severity settings successfully applied to registry?	Select **Yes** to raise an event if AppManager agent severity settings are applied to the registry successfully. The default is Yes.
Event severity when settings successfully applied to registry	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager agent severity settings are applied to the registry successfully. The default is 16.

ConfigSiteCommType

Use this Knowledge Script to configure the AppManager Client Communication Manager service, `NetIQccm`, to use an IP address or hostname to communicate with the management server.

By default, the Client Communication Manager service uses an IP address to locate and communicate with the management server. However, in some environments this may present problems. For example, if your management server and managed clients are connected through a remote dialup connection and use DHCP, IP addresses may be assigned dynamically and change from one connection time to the next, or your management server may be installed on a cluster requiring you to use a cluster name rather than a specific IP address. Use this script to change the default setting for the CCM service.

Configuring AppManager services to use an IP address or hostname is done on a site-by-site basis.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Use IP address to communicate with management server?	Select **y** to have the `NetIQccm` service use an IP address to establish communication with the management server. Select **n** to have the `NetIQccm` service connect to the management server using a hostname. The default is y.
Raise event if communication configuration succeeds?	Select **y** to raise an event indicating the success of the operation. The default is n.
Event severity when job...	Set the event severity level, from 1 to 40, to reflect the importance of the event when the attempt to set the method used by the agent service to communicate with the management server: **... succeeds**. If you set this script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). **... fails**. The default is 5 (red event indicator).

ConfigSiteNetFlowCtrl

Use this Knowledge Script to configure the characteristics of NetIQ Corporation AppManager Client Communication Manager service (`NetIQccm`) communication to the management server for the current repository.

This script allows you to control the flow of network traffic from a managed client to the management server by defining upper and lower bandwidth limits for the size of message batches transferred. One batch is sent at each communication interval. You can also set the length of the communication interval in seconds.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Network flow upper limit	Specify an upper bandwidth limit, in KB, for each network message batch from NetIQccm to the management server. The default of 0 indicates no upper limit.
Network flow lower limit	Specify a minimum bandwidth, in KB, for each network message batch from NetIQ Corporationccm to the management server. The default of 0 indicates no lower limit.
Communication interval	Specify the frequency (in seconds) with which NetIQccm can send message batches to the management server. The default is 0 indicates no delay between message batches.
Tune network flow dynamically?	Select **y** to have the `NetIQccm` agent service dynamically tune and control the size of network message flows to the management server, based on the management server's current load. The default is n.
Raise event if job succeeds?	Select **y** to raise an event indicating the success or failure of the operation. The default is n.
Event severity when job...	Set the event severity level, from 1 to 40, to reflect the importance when the job: **... succeeds**. If you set this script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). **... fails**. The default is 5 (red event indicator).

Example of How this Script Is Used

This script is intended to help you manage network bandwidth and control and tune the transfer of data from managed clients to the management server to suit your network capacity. Using this script, you can restrict the amount of data the `NetIQccm` agent service sends at any one time, as well as the frequency of data transfers.

For example, assume you define an upper limit of 100K, a lower limit of 2K, and a communication interval of one hour (3600 seconds). With this configuration, `NetIQccm` sends up to 100K of data per hour to the management server until the data waiting to be transferred falls below 2K. `NetIQccm` then stores the data in the local repository. At the next interval, if the data to be transferred is greater than 2K, `NetIQccm` resumes sending the data to the management server. If the data package is still below 2K, `NetIQccm` continues to store the data in the local repository until the next interval.

"Dynamic tuning" provides additional flexibility by allowing `NetIQccm` to respond to load changes on the management server. When the *Tune network flow dynamically?* parameter is enabled and the management server becomes busy, `NetIQccm` decreases the amount of data sent and increases the communication interval until the load on the management server is reduced.

Each time the `NetIQccm` service connects to transfer data, it checks the current load on the management server. If load has increased, `NetIQccm` further reduces the amount of data sent in each batch. `NetIQccm` continues to reduce the amount of data sent until the amount of data to be sent falls below the lower limit you set, or until load on the management server decreases, freeing up bandwidth.

DBHealth

Use this Knowledge Script to monitor SQL Server resources associated with the AppManager repository, including:

- The percentage of database space and log space used.
- The time it takes a SQL command or query to execute.
- The status of AppManager scheduled tasks (SQL Server Agent jobs that operate on the AppManager repository).

You can set a threshold for each database resource monitored. If any threshold is exceeded, an event is raised. In addition, you can use this script to check whether any SQL Server services are stopped, and whether AppManager scheduled tasks have failed to run or have been disabled. You can optionally restart services and re-enable scheduled tasks.

This script requires the SQL Server system administrator (`sa`) account or an account with `sa` privileges to run.

If you implement any responsive actions in conjunction with this script, you should set the Location of the actions to **MC**, so they run as managed client actions and are executed even if the management server is not connected to the AppManager repository.

Note
This script supports the monitoring of AppManager agents and AppManager repositories at version 6.0 or later.

Resource Object

SQL Server where the AppManager repository is installed.

Default Schedule

The default interval for this script is **Every 10 minutes**.

This script checks the `sysjobschedules` table in the `msdb` database to determine the last execution time of each SQL Server Agent job that operates on the AppManager repository. The `sysjobschedules` table is updated at 20-minute intervals, and so running this script at more frequent intervals does not yield more timely information about the failure of SQL Server Agent jobs.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if SQL services are down?	Select **Yes** to raise an event if any SQL Server services are detected as down. The default is Yes. **Note** If SQL Server services are not running, the other elements of database health cannot be monitored and the associated events cannot be raised.
Event severity when a service is down	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

Parameter	How to Set It
Raise event if service was shut down normally?	Select **Yes** to raise an event when a service is stopped in a normal manner (for example, by a user or as the expected result of another service being stopped). The default is Yes.
Event severity when service was shut down normally	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 30 (blue event indicator).
Raise event if service is started?	Select **Yes** to raise an event if the script successfully restarts a stopped service. The default is unchecked. **Note** This parameter is effective only when the *Start Down Services* parameter is also Select Yes.
Event severity when attempt to start service fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10 (red event indicator).
Event severity when service started	Set the severity level, from 1 to 40, to indicate the importance to the event. The default is 25 (blue event indicator).
Raise event if service is missing?	Select **Yes** to raise an event when a SQL Server service is not installed in the computer. The default is unselected.
Event severity when service is missing	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 8 (red event indicator).
Raise event if service is disabled?	Select **Yes** to raise an event when a SQL Server service is disabled. The default is unselected.
Event severity when service is disabled	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 12 (yellow event indicator).
Raise event if database space usage exceeds threshold?	Select **Yes** to raise an event when the *Maximum used database space* threshold has been exceeded. The default is unselected.
Event severity when database space usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).
Raise event if log space usage exceeds threshold?	Select **Yes** to raise an event when the Log space utilization threshold has been exceeded. The default is Yes.
Event severity when log space usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).
Raise event if management server not connected?	Select **Yes** to raise an event if the AppManager management server is not connected to the AppManager repository. The default is Yes.
Event severity when management server not connected	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).
Raise event if AppManager SQL jobs disabled?	Select **Yes** to raise an event when any SQL Server Agent job that operates on the AppManager repository has been disabled. The default is Yes.
Raise event if attempt to enable SQL job succeeds?	Select **Yes** to raise an event when a disabled SQL Server Agent job that operates on the AppManager repository is successfully enabled. The default is unchecked.
Event severity when attempt to enable SQL job fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

Parameter	How to Set It
Event severity when attempt to enable SQL job succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).
Raise event if AppManager SQL jobs are not running as scheduled?	Select **Yes** to raise an event when a SQL Server Agent job that operates on the AppManager repository does not run as scheduled. The default is Yes.
Event severity when attempt to retrieve SQL job status fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).
Event severity when SQL job fails to run	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).
Raise event if query process time exceeds threshold?	Select **Yes** to raise an event when the run time for a SQL Server command or query exceed the *process run time threshold*. The default is Yes.
Event severity when query process time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10 (red event indicator).
Event severity when attempt to retrieve query process time fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10 (red event indicator).
Raise event if AppManager repository not found?	Select **Yes** to raise an event if no AppManager repository can be located on the SQL Server on which the script is running. The default is unselected.
Event severity when AppManager repository not found	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 20 (yellow event indicator).
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of the event raised when the script fails to run properly. The default is 5 (red event indicator).
Data Collection	
Collect data for database space utilization?	Select **Yes** to collect data for charts and reports. If enabled, returns the percentage of used database space. The default is unselected.
Collect data for log space utilization?	Select **Yes** to collect data for charts and reports. If enabled, returns the percentage of used log space. The default is unselected.
Collect data for management server connection status?	Select **Yes** to collect data for charts and reports. If enabled, returns the status of the management server connection to the AppManager repository. Returns either: **100** -- management server is connected; or **0** -- management server is not connected. The default is unselected.
Collect data for service status?	Select **Yes** to collect data regarding the up/down status of SQL Server services. The values returned are set in the following parameters: Data value - Service up Data value - Service down The default is unselected.
Collect data for dependent services?	Select **Yes** to also collect data for any services that are dependent on the monitored SQL Server services. The default is unselected.
Monitoring	

Parameter	How to Set It
SQL username	Specify the database user login account that you want to use to access SQL Server. This script requires the "sa" account or an account that has admin group privileges on the target SQL Server. If you want to use a login account other than sa, use the AppManager Security Manager to identify the account. The default is sa. **Note** If you are monitoring SQL Server 7, you need to use a sysadmin role account.
Threshold -- Maximum database space utilization	Specify a threshold for the maximum percentage of database space that can be used before an event is raised. The default is 90%.
Threshold -- Maximum log space utilization	Specify a threshold for the maximum percentage of log space that can be used before an event is raised. The default is 80%.
Enable disabled SQL jobs?	Select **Yes** to enable SQL Server Agent jobs that have been disabled. The default is Yes.
Threshold -- Maximum process run time	Specify the maximum number of seconds allowed for process run time (the time it takes a SQL command or query to complete) before an event is raised. The default is 30 seconds.
Start services if down?	Select **Yes** to start any SQL Server service that is stopped. The default is Yes.
Start dependent services?	Select **Yes** to also start any services that are dependent on SQL Server services started by the script. The default is Yes.
Restart service if shut down normally?	Select **Yes** to start services that were shut down under normal circumstances (for example, by a user or as the expected result of another service being stopped). The default is Yes.
Service start timeout	Specify the number of seconds the script should attempt to start a down service before timing out. The default is 30 seconds.

Example of How this Script Is Used

This script enables you to monitor the AppManager repository for conditions that may cause abnormal operation or result in database consistency problems. This script also helps you monitor the growth and sizing requirements for the AppManager repository so you can plan for changes to your database configuration or your site configuration.

For example, as you monitor more servers and more applications in your environment, or as you gather more data and generate more events, this script monitors the repository to be sure you have the resources to accommodate the increase. If you find you are exceeding any threshold, it may indicate that you should change your database configuration options, for example, to increase the maximum number of user connections or the size of tempdb.

If you continue to see events or see the events indicate heavy work load (for example, longer query execution times), you may need to consider splitting your site by installing additional management servers and repositories or freeing up space on your repository server by moving the AppManager management server and repository components onto separate computers.

DeleteExpiredReports

Use this Knowledge Script to delete expired reports generated by an AppManager report agent. If you have configured more than one report agent to generate reports to the same location, run this script on one of the report agents to delete all expired reports.

Resource Object

Report agent

Default Schedule

The default interval for this script is **Run once**.

You can set the schedule to periodically check for expired reports.

Setting Parameter Values

Set the following parameters as needed:

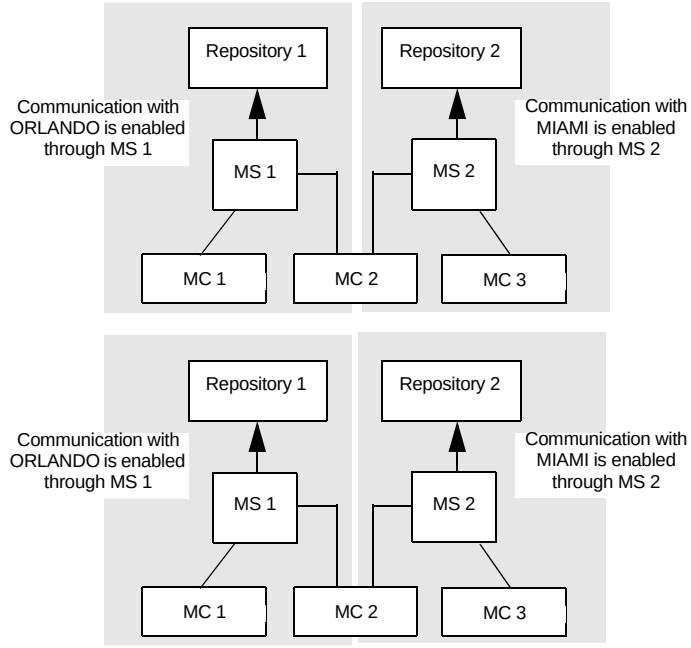
Parameter	How to Set It
Raise event if report successfully deleted?	Select **y** to raise an event if expired reports are deleted. The default is y.
Generate deletion report?	Select **y** to generate a report detailing which reports were deleted. The default is y.
Include parameter table?	Select **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is DeleteExpRpts.
Add job ID to output folder name?	Select **y** to append the job ID to the name of the output folder. The default is n. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Expired Reports Deleted.
Add timestamp to title?	Select **y** to append a timestamp to the title of the report, making each title unique. The default is n. A timestamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event severity when report successfully generated	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Event severity when report generation fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

DisableSiteComm

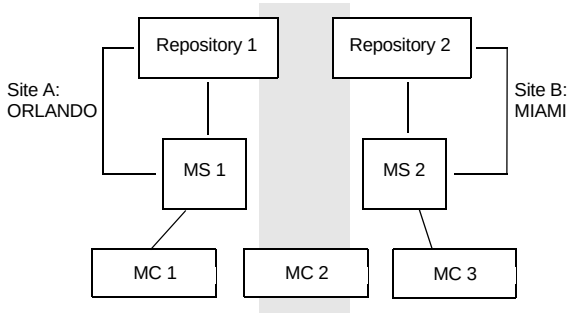
Use this Knowledge Script to temporarily disable network communication from a managed client on Windows to the repository. All messages, including events, data, and job status, are saved in the local repository of the managed client until network communication is re-enabled, at which point it is transferred to the management server. The size of message batches and frequency of delivery can be controlled through the ConfigSiteNetFlowCtrl script.

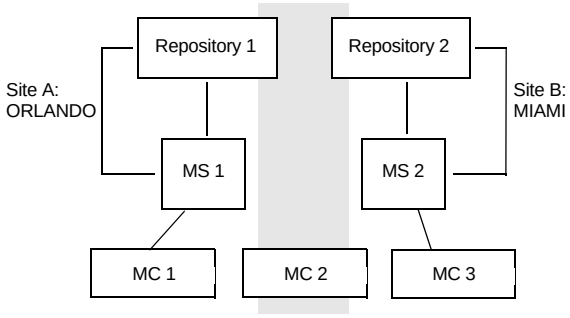
If a managed client is managed by more than one site (that is, if information for the managed client is stored in more than one repository) you can set *Disable communications for all sites* to **y** to disable communication from the managed client to all repositories with which the managed client communicates.

In this simplified example, MC 2 normally sends data and events to both `ORLANDO` and `MIAMI`.



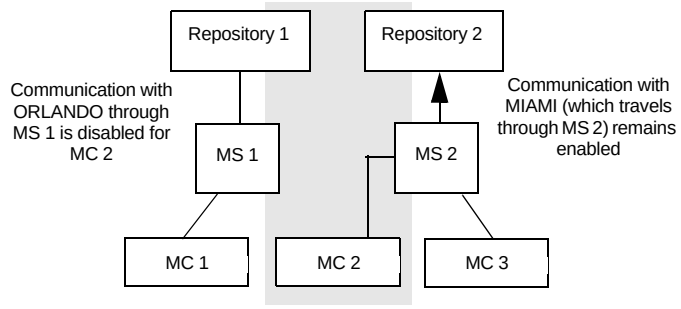
If you run this script on MC 2 and enable the *Disable communications for all sites* parameter, communication to both `ORLANDO` (Repository 1) and `MIAMI` (Repository 2) is disabled for MC 2. Communications by MC 1 and MC 3 are not affected.

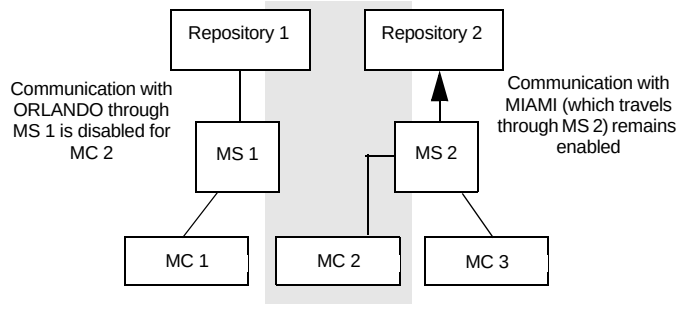




You can set the *Disable communications for all sites* parameter to **n** to disable communication from the managed client only to the repository you are currently logged onto.

For example, you have logged onto Repository 1 in the AppManager Operator Console (in the Login dialog box). You run this script on MC 2 and set *Disable communications for all sites* to **n**. Communication between MC 2 and Repository 1 is disabled, but communication between MC 2 and Repository 2 is unaffected. Communications by MC 1 and MC 3 are also unaffected.





Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Disable communications for all sites?	Select **y** to disable communication between the managed client and the repositories with which it communicates. Select **n** to disable communication from the managed client to the repository you are logged onto. The default is n.
Raise event when attempt to disable communication succeeds?	Select **y** to raise an event indicating the success of the operation. An event is always raised when the job fails. The default is n.
Event severity when attempt to disable communication...	Set the event severity level, from 1 to 40, to reflect the importance when the job: **... succeeds**. If you set this script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). **... fails**. The default is 5 (red event indicator).

Example of How this Script Is Used

This script lets you intentionally stop the communication between managed clients and repositories. For example, if you are experiencing network problems, you may want to temporarily disable communication while you troubleshoot the problem.

You can also force data and events be stored in the local repository. For example, if you are experiencing high network activity, you can disable communication between the managed client and the management server and store data locally until the demand for server bandwidth is reduced. To set up a regular schedule for uploading events or data from the local repository, use the SiteSchedUpload script.

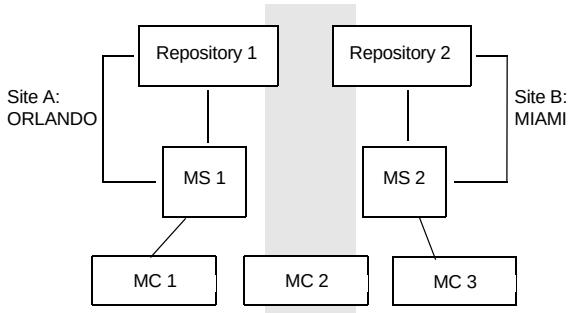
EnableSiteComm

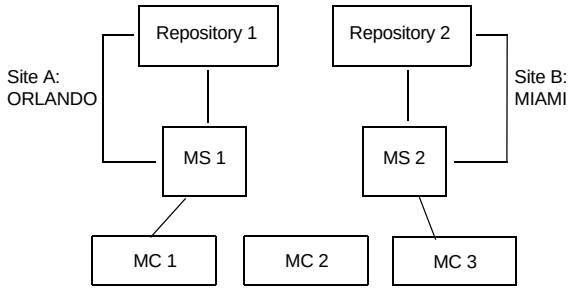
Use this Knowledge Script to resume regular ongoing network communication from a managed client to the management server. Network communication may be disabled because you have run the DisableSiteComm script to disable network communication between the managed client and management server.

As soon as network communication is restored, any information temporarily stored in the local repository of the managed client while communication was disabled is transferred to the management server, either immediately or in the next scheduled upload if the managed client is configured to transfer events or data according to a schedule.

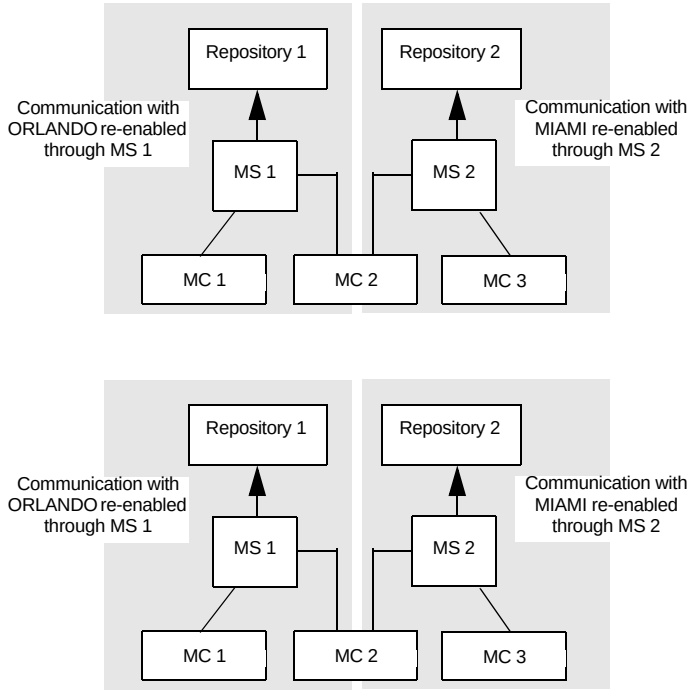
If a managed client is managed by more than one site (that is, if information for the managed client is stored in more than one repository) you can set the *Enable communications for all sites* parameter to **y** to enable communication from the managed client to all management sites with which the managed client communicates.

In this simplified example, MC 2 normally sends data and events to both `ORLANDO` and `MIAMI`, but communication with these sites has been temporarily disabled for this managed client.



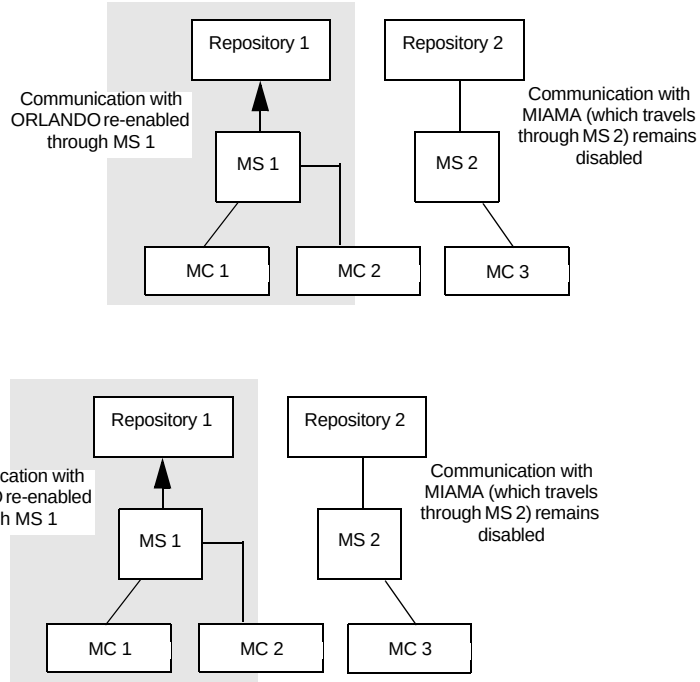


If you run this script on MC 2 and enable the *Enable communications for all sites* parameter, communication to both `ORLANDO` (Repository 1) and `MIAMI` (Repository 2) is re-enabled for MC 2.



You can set *Enable communications for all sites* to **n** to enable communication from the managed client only for the repository you are currently logged onto.

For example, if you have logged onto Repository 1 in the AppManager Operator Console (in the Login dialog box), and run this script on MC 2 with *Enable communications for all sites* Select **n**, communication between MC 2 and Repository 1 is enabled, but communication between MC 2 and Repository 2 remains disabled.



Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Enable communications for all sites?	Select **y** to enable communication from the managed client to all repositories the managed client communicates with Select **n** to enable communication from the managed client to the repository you are logged onto. The default is n.
Raise event when attempt to enable communication succeeds?	Select **y** to generate an event indicating the success or failure of the operation. The default is n.
Event severity when attempt to enable communication...	Set the event severity level, from 1 to 40, to reflect the importance when the job: **... succeeds**. If you set this script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). **... fails**. The default is 5 (red event indicator).

GreyMachines

Use this Knowledge Script to monitor AppManager agents that have gone "grey," in other words, that are not responding to management server Ping requests. This script raises an event if the number of unresponsive agents exceeds the threshold you set.

Note
This script supports AppManager repositories of version 6.0 and later.

Resource Object

SQL Server folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if agents are not responding?	Select **Yes** to raise an event when an agent has gone "grey"--does not respond to a Ping from the management server. The default is Yes.
Event severity when agents are not responding	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).
Raise event if repository is offline or unavailable?	Select **Yes** to raise an event when repository is offline or unavailable. The default is Yes.
Event severity when repository is offline or unavailable	Set the severity level, from 1 to 40, to indicate the importance of the event raised when the repository is offline or unavailable. The default is 10 (red event indicator).
Data Collection	
Collect data for unresponsive agents?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of agents that do not respond to a Ping from the management server. The default is unselected.
Monitoring	
SQL username	Provide the user name for the SQL Server account to use to connect to the AppManager repository. If you leave this parameter blank, the script uses the account under which the `NetIQ AppManager Client Resource Monitor` service is running. The default is `sa`. **Note** The password for a SQL Server account must be stored in the AppManager repository. Use AppManager Security Manager to enter SQL Server security information into the AppManager repository.
AppManager repository name	Provide the name of the AppManager repository you want to monitor for unresponsive agents. The default is `QDB`.
Threshold -- Maximum number of unresponsive agents	Set a threshold for the maximum number of unresponsive agents allowed before an event is raised. The default is 0 nonresponsive agents.

Parameter	How to Set It
SQL Server connection timeout	Set an amount of time, in seconds, that the script should wait to get a response from the AppManager repository server when attempting to retrieve the list of “grey” (unresponsive) agents before timing out. The default is 10 seconds.
SQL Server connection retry attempts	Set the number of times the script should retry the attempt to connect to the AppManager repository after a connection timeout occurs. The default is 1 attempt.

IISContinueSite

Use this Knowledge Script to continue a paused IIS site remotely. If the script is unable to continue a paused IIS site, an event is raised.

This script is not supported on IIS version 7.x.

Resource Objects

Servers running Windows Server 2003 or Windows XP Professional

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if operation succeeds?	Select **Yes** to raise an event if the attempt to continue the site succeeds. The default is Yes.
Event severity if operation succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue event indicator).
Raise event if operation fails?	Select **Yes** to raise an event if the attempt to continue the site fails. The default is Yes.
Event severity if operation fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 15 (yellow event indicator).
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator). This script raises an event for unexpected script errors. For example, if a script aborts before the job starts or during the job, an event is raised.

IISPauseSite

Use this Knowledge Script to temporarily pause an IIS site. If the IIS site cannot be paused, an event is raised. This script raises an event if the script is unable to continue a paused IIS site.

This script is not supported on IIS version 7.x.

Resource Objects

Servers running Windows Server 2003 or Windows XP Professional

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if operation succeeds?	Select **Yes** to raise an event if the attempt to pause the site succeeds. The default is Yes.
Event severity if operation succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue event indicator).
Raise event if operation fails?	Select **Yes** to raise an event if the attempt to pause the site fails. The default is Yes.
Event severity if operation fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 15 (yellow event indicator).
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator). This script raises an event for unexpected script errors. For example, if a script aborts before the job starts or during the job, an event is raised.

IISRestartServer

Use this Knowledge Script to stop and then restart an IIS server. This script raises events if the attempt to stop or restart a service fails or succeeds. You can detect and start any service that was stopped abruptly.

Resource Objects

For AppManager version 7.x: Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows Server 2003 and Windows XP Professional

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if attempt to restart server succeeds?	Select **Yes** to raise an event if the attempt to restart the IIS server succeeds. The default is Yes.
Event severity if operation succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue event indicator).
Raise event if attempt to restart server fails?	Select **Yes** to raise an event if the attempt to restart the IIS server fails. The default is Yes.
Event severity if server start fails	Set the severity level, from 1 to 40, to indicate the importance of the event. This Knowledge script raises this event when the attempt to start the IIS server fails. The default is 5 (red event indicator).
Event severity if server stop fails	Set the severity level, from 1 to 40, to indicate the importance of the event. This Knowledge script raises this event when the attempt to stop the IIS server fails. The default is 5 (red event indicator).
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator). This script raises an event for unexpected script errors. For example, if a script aborts before the job starts or during the job, an event is raised.
Administration	
Restart the server?	Select **Yes** to restart the IIS server, after it is stopped. The default is Yes.
Service start/stop delay	Set the number of seconds to wait after the IIS server is stopped before attempting to automatically restart it. The default waiting time is 30 seconds.
Restart dependent services? (6.0+)	Select **Yes** to restart any services that depend on the server you stopped. The default is Yes. **Note** Dependent services are restarted only by AppManager agents version 6.0 and later.
Service start/stop retry count	Set the number of times to attempt to restart a service after it has stopped. The script attempts to restart a service 3 times (default).

IISRestartSite

Use this Knowledge Script to shut down and restart an IIS site instance. This script raises an event if the IIS site cannot be shut down or restarted.

Resource Objects

For AppManager version 7.x: Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows Server 2003 and Windows XP Professional

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if operation succeeds?	Select **Yes** to raise an event if the attempt to restart the IIS site succeeds. The default is Yes.
Event severity if operation succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue event indicator).
Raise event if operation fails?	Select **Yes** to raise an event if the attempt to restart the IIS site fails. The default is Yes.
Event severity if operation fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 15 (yellow event indicator).
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator). This script raises an event for unexpected script errors. For example, if a script aborts before the job starts or during the job, an event is raised.
Administration	
Restart site after shutdown?	Select **Yes** to restart the site after shutdown. The default is Yes.

LRReadParameters

Use this Knowledge Script to view local repository (LR) configuration information on a managed client computer. You can specify the LR parameter or parameters you want to view, or view all parameters. This script raises an event each time you run the job, and the event details display the name and value of each parameter.

LR information consists of parameter values that are stored in the local repository. You can use this script in conjunction with AppManager *_Config* scripts (for example, General_ConfigMachineDown, NT_ConfigServiceDown) to read the configuration information written in the local repository by the *_Config* scripts.

LR information can be stored in the local repository by using the LRWriteParameters Knowledge Script.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if LR configuration retrieved successfully?	Select **Yes** to raise an event if the script is successful in accessing the local repository and reading the parameter values. The default is Yes.
Event severity when LR configuration retrieved successfully	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15 (yellow event indicator).
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator). This script raises an event for unexpected script errors. For example, if a script aborts before the job starts or during the job, an event is raised.
Administration	

Parameter	How to Set It
Retrieve all LR parameters?	Select **Yes** to retrieve all LR information in the AppManager agent's local repository. The default is Yes. If you clear this check box, you must specify the name of the parameter or parameters you want to retrieve. For example, if there are two parameters in the local repository, **name** and **location**, to read the value for **location**, specify **location** in any of the *Parameter#* parameters. This script can read the value of up to 20 specified parameters each time you run the script.
Parameter 1 ... 20	Specify the name of the parameter or parameters you want to retrieve. Enter the parameter name without quotes. For example, if there are two parameters in the local repository, **name** and **location**, to read the value for **location**, specify **location** in any of the **Parameter#** parameters. If you clear the *Retrieve all LR parameters?* check box, you must specify the parameter names. This script can read the value of up to 20 specified parameters each time you run the script.

LRRemoveParameters

Use this Knowledge Script to remove local repository (LR) configuration information from a managed client computer. Specify the parameter or parameters you want to remove, or remove all parameters from the local repository. This script raises an event each time you run the job. The event details display information about the parameters that were removed.

LR information consists of parameter values that are stored in the local repository. You can use this script in conjunction with the AppManager *_Config* scripts (for example, General_ConfigMachineDown, NT_ConfigServiceDown) to remove the configuration information entered by the *_Config* scripts from the local repository.

To view LR information that is stored in the local repository, use the LRReadParameters script.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if parameters deleted successfully?	Select **Yes** to raise an event if the script is successful in removing the parameter values. The default is Yes.
Event severity when parameters deleted successfully	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15 (yellow event indicator).
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator). This script raises an event for unexpected script errors. For example, if a script aborts before the job starts or during the job.
Administration	

Parameter	How to Set It
Delete entire LR?	Select **Yes** to remove all LR information from the AppManager agent's local repository. The default is unselected. If you select this check box, you must specify the name of the parameter or parameters you want to remove. For example, if there are 2 parameters in the local repository, **name** and **location**, to remove the **location** parameter, specify **location** in any of the *Parameter#* parameters. This script can remove up to 20 specified parameters each time you run the script.
Parameter 1 ... 20	Specify the name of the parameter or parameter you want to remove. Enter the parameter name without quotes. For example, if there are 2 parameters in the local repository, **name** and **location**, to remove the **location** parameter, specify **location** in any of the *Parameter#* parameters. If you select the *Delete entire LR?* parameter, you must specify the parameter names. This script can remove up to 20 specified parameters each time you run the script.

LRWriteParameters

Use this Knowledge Script to store local repository (LR) configuration information in a managed client computer. You can specify a name and value for each parameter you want to store. This script raises an event each time you run the job. The event details display information about the parameters that were set.

LR information consists of parameter values that are stored in the local repository. You can use this script to enter your own information into the local repository for use by custom or customized scripts.

This script contains the same capabilities as AppManager *_Config* scripts, except that you can write any named/value pair to the local repository as opposed to specifically named entries. You can use this script instead of the *_Config* scripts when you use the following named entries (shown with their matching *_Config* scripts):

Named Entry	Knowledge Script
_NQ_PingMachine_MachineList	Client_ConfigPingMachine
_NQ_PingMachine_MachineFile	Client_ConfigPingMachine
_NQ_MachineDown_MachineList	General_ConfigMachineDown
_NQ_MachineDown_MachineFile	General_ConfigMachineDown
_NQ_RemoteService_MachineList	NT_ConfigRemoteServiceDown
_NQ_RemoteService_MachineFile	NT_ConfigRemoteServiceDown
_NQ_RemoteService_ServiceList	NT_ConfigRemoteServiceDown
_NQ_Service_ServiceList	NT_ConfigServiceDown
_NQ_Service_ExcludeList	NT_ConfigServiceDown

To remove LR information from the local repository, use the LRRemoveParameters Knowledge Script.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Create event if LR set successfully?	Select **Yes** raise an event if the script is successful in setting local repository configuration information. The default is Yes.
Severity - LR set successfully	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15 (yellow event indicator).

Parameter	How to Set It
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator). This script raises an event for unexpected script errors. For example, if a script aborts before the job starts or during the job.
Administration	
Overwrite value if it already exists?	Select **Yes** to overwrite a parameter value if it already exists in the AppManager agent's local repository. The default is Yes. **Note** This script is not case-sensitive.
Parameter 1 ... 20	Provide the name and value for each parameter you want to set. Enter the parameter name without quotes. For example, to create a **location** parameter and set it to **San Jose**, under any *Parameter#* parameter, specify **location** in **Name** and **San Jose** in **Value**. If the **location** parameter already exists, by default, the value is overwritten. This script can set up to 20 specified parameters each time you run the script.

MonitorMSCommunications

Use this Knowledge Script to monitor secure agent communications with the management server.

This script monitors the Windows Application log for events that indicate a mismatch of the encryption key used by the agent (on the monitored computer) and the management server.

This script runs continuously and raises an event when a key mismatch is detected.

Note
Run this script on computers where the management server is installed.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Asynchronous**.

Setting Parameter Values

Set the following parameter as needed:

Parameter	How to Set It
Event severity when key mismatch detected	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

MSHealth

Use this Knowledge Script to monitor for self-monitoring events associated with the managed client, Client Communication Manager agent service, and management server. It looks in the Windows Application log for events of several types: general, communication, job, security, and upgrade.

You can filter event log entries by event type and by specifying a combination of include and exclude strings for each event field. All event log entries that match the filtering criteria are returned in the event detail message. An event is raised anytime AppManager places a self-monitoring event in the Windows Application log.

Run this script on computers where the management server is installed. To check for self-monitoring events on computers that do not have the management server installed, use the AgentHealth script.

Resource Object

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Asynchronous**.

Regardless of the schedule you select, once you start the script, its job status appears as **Running**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Monitor events of type...	Select **y** to raise an event when AppManager places a self-monitoring event in the Windows Application Log of any of the following types: **... general**. The default is y. **... communications**. The default is y. **... job**. The default is y. **... security**. The default is y. **... upgrade**. The default is y.
Event severity for events of type...	Set the event severity level, from 1 to 40, to reflect the importance when the following types of event are inserted in the Windows event log: **... general**. The default is 15 (yellow event indicator). **... communications**. The default is 15 (yellow event indicator). **... job**. The default is 15 (yellow event indicator). **... security**. The default is 15 (yellow event indicator). **... upgrade**. The default is 15 (yellow event indicator).

Parameter	How to Set It
Filter events by event description	The script will look for matching entries in the event log Description field. Multiple strings can be entered separated by commas. The filter string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary. For example, to include “communication” and “cold start” event types but exclude them when associated with the managed client or CCM agent service, type: communication,cold start:mc,ccm
Use case-sensitive description filter?	Select **y** to make all filter statements for this script case-sensitive. The default value is n (not case-sensitive).

RemovePrimaryMS

Use this Knowledge Script to remove the agent's designated primary and secondary management servers. This script removes the designations for the current site. To remove designations for another site, you must run this script from that site.

For performance reasons, you should always designate an agent's primary management server and if there is one, a secondary management server, within a site. To change the management server designations for an agent, use the SetPrimaryMS script.

This script does not change the authorized list of management servers with which the agent can communicate.

Before using this script, make sure the agent is configured to authorize communication with a management server by running the AgentConfigMSRestrictions Knowledge Script. If the agent is not authorized to communicate with a management server and you remove the agent's management server designations, the client computer cannot communicate with AppManager. To resolve this problem, you must manually edit the registry on the managed client computer to specify an authorized management server list in the `\HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\4.0\NetIQMC\Security\AllowMS`.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when primary and backup management server setting removed?	Select **y** to raise an event when the managed client's primary and secondary (backup) management servers have been successfully removed. An event is always raised if the job fails. The default is n.
Event severity when primary and backup management server setting is removed	Set the event severity level, from 1 to 40, to indicate the importance of the event when the job completes successfully. The default severity level is 25 (blue event indicator).

SchedMaint

Use this Knowledge Script to specify a period of scheduled maintenance for an application resource (such as WMI) or all resources on a managed client computer on Windows. During the maintenance period, regularly scheduled AppManager jobs for the application resource do not run. You can specify the application resources you want to block by script category, or prevent all jobs from running on a server (for example, because of expected downtime).

This icon,  , indicates that a Windows computer is in maintenance mode, or all application resources on a computer are in scheduled maintenance mode. It indicates that AppManager has temporarily stopped monitoring the computer.

- The icon is displayed next to all resources when all application resources for a computer are in scheduled maintenance mode or when a computer is in machine maintenance mode.
- The icon is displayed next to all resource objects on a computer when a particular application resource is in scheduled maintenance mode. Only jobs for the specified application resource are blocked.

You define the start and end time for the scheduled maintenance period under the **Schedule** properties tab. This script does not support a start date in the future for agents earlier than AppManager 6.0. Jobs resume running on the managed computer when the maintenance period expires.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Daily**. However, you should use the Schedule tab to set a schedule appropriate to your environment and maintenance needs.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Knowledge Script category to block (e.g., SQL)	Specify the script category for the jobs you do not want to run during a maintenance period (for example: sql). You can specify either a single category or an asterisk (*) for all jobs. The default is all jobs (*).
Raise event when schedule implementation succeeds?	Select **y** to generate an event indicating the success or failure of the operation. The default is n.
Event severity when schedule implementation succeeds	Set the event severity level, from 1 to 40, to indicate the importance of a successful registration of the management server. The default severity level is 25 (blue event indicator).

Example of How this Script Is Used

In many environments, specific application servers have regularly scheduled periods when they are brought down by administrators so administrative tasks can be performed.

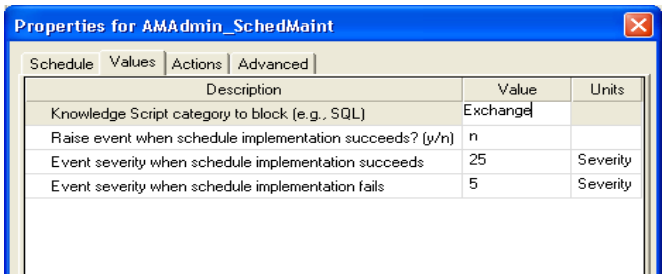
For example, an organization may have 20 Exchange servers that are shut down every Friday at 9 P.M. This interruption causes all of the AppManager Exchange jobs that are not explicitly stopped to error out and forces the administrator to restart the jobs manually when the servers are brought back online.

With this script, administrators can define a specific schedule for temporarily blocking jobs during a planned maintenance period.

Using the Exchange example above, you might set a start time of 8:55 p.m. and an end time of 2:55 a.m. on the Schedule tab. Click **Every** in the Frequency section to set an **End** time. The frequency interval (such as 5 Minutes) is ignored.

On the Values tab, you might identify **exch** (if only Exchange is going to be off-line) or * (if the computers are going to be physically shut down) as the script category to block on the Values tab.

For example, to block Exchange Knowledge Script jobs, you might set the parameters on the Values tab similar to the following example:



At 8:55 p.m. local time (where the job is running), all Exchange Knowledge Script jobs running on the target computers are stopped. At 2:55 a.m. local time, the maintenance period expires and the Exchange jobs resume running at their regularly scheduled intervals.

SetAllowMS

Use this Knowledge Script in sites with multiple management servers or multiple repositories to restrict the management servers that can control the agent.

This script sets a registry entry on the agent computer to explicitly allow a managed client to communicate with specified management servers from other management sites. The list of management servers with which the agent communicates is stored in the following registry key:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\4.0\NetIQMC\Security\AllowMS
```

An asterisk (*) as a value for the `AllowMS` registry key authorizes all management servers to communicate with the agent. With this setting, "anonymous" management servers, servers with which the agent has not explicitly authorized communication, can communicate with the agent. This represents the lowest-security setting. It is the default if you do not choose to designate a primary management server during agent installation.

This script should not be used to enforce security or control communication between the management server and the managed client within a single site. Within a site, you should designate a primary and, if desired, a secondary management server for each agent. A separate registry key is involved in those designations; you can use the SetPrimaryMS Knowledge Script to identify the primary and secondary management server for each managed client within sites where more than one management server is installed.

You can specify the hostnames of allowed management servers for the *New hostname(s) for AllowMS* parameter. The computers you specify here will not become the agent's primary or secondary management server, but those computers can communicate with the agent and instruct it to run monitoring jobs.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
New hostname(s) for AllowMS	Specify a comma-separated list of computer hostnames to designate the management servers that are allowed to communicate with this agent. The `AllowMS` registry key will be set with this list as the value. **Note** it is a good idea to use this script to allow management servers from other management sites to use this agent. For management server-to-agent communications within a single site, use the SetPrimaryMS Knowledge Script.

Parameter	How to Set It
Raise event if attempt to set AllowMS succeeds?	Select **y** to raise an event if the job succeeds. The default is y.
Event severity when attempt to set AllowMS succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue event indicator).

SetDataTimeStamp

Use this Knowledge Script to set the timestamp for data as it is referenced for reports. This setting affects all reports, but it does not affect areas other than reporting.

You can set one of three timestamps:

- **AppManager Repository** uses the local date/time of the AppManager repository computer.
- **Agent** uses the local date/time of the AppManager agent computer.
- **Custom** uses UTC (Coordinated Universal Time) plus or minus *N* hours.

By default, AppManager reports use the local time of the AppManager repository from which the reports are generated. Under circumstances where you want to have an AppManager repository-centric view of your data, you can leave these settings at their defaults.

Under circumstances where the accuracy of your reports depends on data being understood in the context of the local times during which it was collected, you would want to use the **Agent** timestamp. For example, if you are collecting data in four different time zones and want your report to include only data collected between 8 AM and 5 PM, you need that time frame to be relative to each time zone.

If you need to see all your data in the context of a specific time zone, you can use the **Custom** setting, and set the time zone by specifying the number of hours in positive or negative relation to UTC.

Resource Object

Report agent

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if timestamp successfully set?	Select **y** to raise an event if a timestamp is set successfully. The default is y.
Set timestamp to	Select a timestamp to use in reports: • **AppManager Repository** to set the timestamp to the local time of the AppManager repository. • **Agent** to set the timestamp to the local time of the AppManager agent that collected the data. • **Custom** to set the timestamp to a custom time (UTC plus or minus *N* hours). If you select this option, you must specify the number of hours in the following parameter.
Custom time bias	Specify the number of hours by which UTC is modified. For example, if you enter 8, the time bias is Select UTC plus 8 hours. If you enter -8, the time bias is Select UTC minus 8 hours. Enter 0 to use UTC time.

Parameter	How to Set It
Event severity when timestamp successfully set	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

SetDeploymentWebService

Use this Knowledge Script to set or change the hostname of the Deployment Web Service with which the managed client should communicate to install the agents remotely.

Note
For details on installing the agents remotely, see the *User Guide for Control Center*.

The Deployment Web Service is normally set during agent installation. If for any reason you did not supply the hostname of the Deployment Web Service during agent installation, or if you need to change the Deployment Web Service that was set for an agent, use this script to set or change it.

The computer that hosts the Deployment Web Service must be accessible over the network via Port 80 to all managed clients.

This script sets the following registry key on the target computer:

```
HKLM\SOFTWARE\NetIQ\AppManager\4.0\AgtShared\DeploymentEndpoint
```

To disable communication with the Deployment Web Service, leave the *Name of Deployment Web Service* parameter blank.

Note
After you run this script, the AppManager agent may take up to six hours to report its software inventory to the deployment Web service. Restart the NetIQ AppManager Client Resource Monitor and NetIQ AppManager Client Communication Manager agent services to ensure that the agent reports its software inventory immediately.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if job succeeds?	Select **Yes** to raise an event if the job succeeds. This script always raises an event if the job fails.
Event severity when job succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue event indicator).
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10 (red event indicator).
Name of Deployment Web Service	Specify the hostname of the Deployment Web Service. To disable remote installation of agents, run the job with this parameter left blank.

SetKSStandby

Use this Knowledge Script to designate a selected managed client as a standby managed client for specified script categories and for the master managed client.

A *standby* managed client runs jobs only when the master managed client is down, or when jobs from the specified script category are blocked.

If a master managed client is currently configured, leave the *Hostname for master managed client* parameter blank to change it.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Knowledge Script categories (comma-separated)	Specify the script categories for which the selected managed client will serve as a standby. Whenever a job from one of these categories cannot run because the agent that is supposed to run it cannot be reached, the job defaults to the standby. Separate the names of multiple script groups with commas and no spaces. The category name is shown on the script view tab for that category. For example, for Microsoft IIS, the category name is "IIS." The default is * (all script categories).
Hostname for master managed client	Designate the master managed client for the script category specified in the previous parameter by supplying its hostname.
Raise event if job succeeds?	Select **y** to raise an event if the job succeeds in designating a master managed client to serve as a standby for the specified script categories. The default is n.
Event severity when job succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue event indicator).

SetLocalRPSize

Use this Knowledge Script to modify the maximum number of events or data points that can be stored in the managed client's local repository. If the managed client is not able to communicate with the management server for any reason, the local repository for the managed client stores the most recent events and data points up to this limit until communication with the management server is restored.

If the number of events or data points exceeds the limit you have set (for example because of an extended network interruption), the oldest events or data records are lost as new events or data points are recorded.

Setting this registry key to 0 may affect the performance on the managed computer when a large number of records are inserted into the local repository (for example, because the management server is down, communication is disabled, or the managed computer is between scheduled uploads). If you are using ODBC, no changes are required.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Change maximum number of data points to store?	Select **y** to change the maximum number of data points that can be added to the local repository. The default is y.
Maximum number of data points to store	Specify the maximum number of data points that can be added to the local repository. Enter 0 if you do not want to set a limit on the maximum number of data points. The default is 10,000 data points.
Change maximum number of events to store?	Select **y** to change the maximum number of events that can be added to the local repository. The default is y.
Maximum number of events to store	Specify the maximum number of events that can be added to the local repository. Enter 0 if you do not want to set a limit on the number of events. The default is 10,000 events.
Raise event if repository configuration succeeds?	Select **y** to raise an event indicating the success or failure of the operation. The default is n.
Event severity when repository configuration...	Set the event severity level, from 1 to 40, to reflect the importance when the job: **... succeeds**. If you set this script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). **... fails**. The default is 5 (red event indicator).

SetPrimaryMS

Use this Knowledge Script to designate the primary and secondary management server for an agent. If the primary management server fails, the secondary, or backup, management server takes over communication with the managed client until communication with the primary management server resumes.

Within an AppManager management site, the agent only accepts job requests and sends events to its designated management server. During installation, you can designate the agent's primary and optionally, a secondary management server. For performance reasons, you should always designate the primary and, if there is one, a secondary management server, within a management site.

After installation, use this script to add a secondary management server, or change the agent's designated primary management server. If you are managing a computer from more than one AppManager site, run this script from another site to designate the primary and secondary management server for that site.

If you are managing a client from more than one management site, run this script from each site to designate the primary and secondary management server for that site. To authorize an agent to communicate with an additional management server, use the AgentConfigMSRestrictions Knowledge Script.

The list of authorized management servers is updated to include the designated primary and secondary management servers. If the agent was configured to not allow anonymous management server communication, that communication restriction goes into effect after you designate the primary and secondary management server.

To improve repository performance, you should always designate a primary management server for each managed client computer in your site. If you cannot designate a primary management server during installation—for example, if the installation program cannot communicate with the management server—you must manually designate the primary management server using this script.

To configure a primary and backup management server for a managed Windows client, run this script and set the *Primary management server hostname* and *Backup management server hostname* parameters. After establishing a primary and backup management server for a managed client, you can also use this script to change the primary management server hostname, the backup management server hostname, or both using the *Select management server operation to perform* parameter:

Designation to Change	How to Change It
The managed client's **primary** management server	Enter a new hostname for the primary management server. Leave the *Backup management server hostname* parameter blank. Set the *Management server operation to perform* parameter to 1.
The managed client's **backup** management server	Enter the hostname of the existing primary management server. Enter a new hostname for the backup management server. Set the *Management server operation to perform* parameter to 2.
Both the **primary** and **backup** management servers	Enter a new hostname for the primary management server. Enter a new hostname for the backup management server. Set the *Management server operation to perform* parameter to 3.

Set the *Management server operation to perform* parameter properly to avoid unexpected behavior. For example, assume you want to establish the computer `BOSTON` as the primary management server, but do not want to make any change to the backup management server. If you run this script with the *Backup management server hostname* blank but inadvertently set the *Management server operation to perform* parameter to 3, the empty *Backup management server hostname* parameter is not ignored. Because you have indicated you want to change both the primary and backup management servers, the blank entry for *Backup management server hostname* is interpreted as authorization for any available management server to act as a backup management server for the target managed client.

For more information about multiple management server configurations, see the *Administrator Guide for AppManager*.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

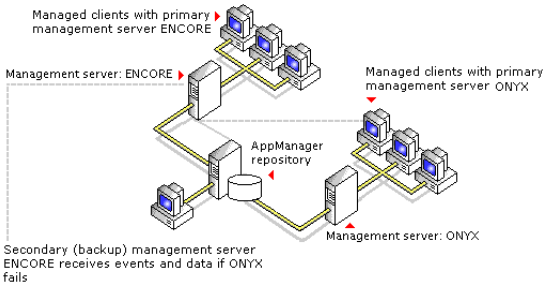
Set the following parameters as needed:

Parameter	How to Set It
Raise event if set operation succeeds or fails?	Select **y** to raise an informational event when the managed client is successfully updated with the new management server information or if the update fails. The default is n.
Event severity when set operation succeeds	Set the event severity level, from 1 to 40, to indicate the importance of a successful registration of the management server. The default severity level is 25 (blue event indicator).
Primary management server hostname	Provide the name of the management server you want to use as the primary management server. **Note** The value for this parameter cannot be blank, even if you are only setting the backup management server.
Backup management server hostname	Enter the name of the management server you want to use as the backup management server.
Management server operation to perform	Specify which management server configuration you want to update for the target managed client. Type: • **1** to change only the primary management server • **2** to change only the backup management server • **3** to change both the primary and backup management servers The default is to change the primary management server (1).

Example of How this Script Is Used

When you install the AppManager agent, you automatically designate a **primary management server**, and that management server becomes the only management server that the managed client communicates with for a single repository/management server configuration. A **secondary** or **backup management server** can also be defined at installation for each managed client in case the primary management server fails. The secondary management server only communicates with the managed client when the primary management server is unavailable. When communication with the primary management server resumes, the managed client resumes exclusive communication with the primary management server.

Because a multiple management server environment is chiefly intended for failover functionality (to provide an alternative management server if the primary management server fails), each managed client can have one primary management server and one backup management server for each repository.



In addition, identifying a specific management server for specific groups of managed clients gives you greater control over the distribution of communication load and network bandwidth usage.

SetReportPaths

Use this Knowledge Script to change the default output path used by the report agent.

You can also use this script to instruct the report agent to display the locations of reports as hyperlinks in events. By default, the absolute path to a report is displayed as text on the **Message** tab of the Event Properties dialog box. Use this script to display a hyperlink to the report in addition to the default text. Clicking the hyperlink opens an instance of Internet Explorer to display the contents of the report.

Resource Object

AM Repositories object under the Report agent

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when change to report path succeeds?	Select **y** to raise an event when one or both of these paths are successfully changed. The default is y.

Base output path	Use this parameter to set a new base output path for the Report Agent.
	Type the path using the following format:
	`\\<server>\<share>\<path to folder>`
	where:
	`<server>` is the computer where you want to write reports.
	`<share>` is the share name of the drive where you want to write reports.
	`<path to folder>` is the absolute path to the folder where you want to write reports.
	For example, the base output path might be:
	`\\RptServer\C$\Program Files\NetIQ\ReportCenter\Web\Report`
	You can also use an absolute path for the value of this parameter. For example:
	`C:\Program Files\NetIQ\ReportCenter\Web\Report`
	Note Leave this parameter blank if you are only using this script to set the *URL mapping* parameter.

URL mapping	Use this parameter to set the URL mapping registry value. Type the URL to the AppManager Web Management Server using the following format: `<protocol name>://<web server name>` where: `<protocol>` is the Internet Protocol, either `HTTP` or `HTTPS`. `<web server name>` is the computer where you have installed the AppManager Web management server. **Note** This parameter should be left blank if you are only using this script to set the *Base output path* parameter. This parameter must be set in order to successfully use Action_SMTPMailRpt.

Parameter	How to Set It
Event severity when change to report path succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Event severity when change to report path fails	Set the event severity level, from 1 to 40, to indicate the importance of the event when the job fails. The default is 5 (red level indicator).

SetResDependency

Use this Knowledge Script to define the resources required to run script jobs on a Windows computer. Resources can include physical file-system related resources such as logical disk drives or directories, or the availability of specific services. You can specify the dependency list by script category or define resources that apply to all script jobs.

The resources and services you specify must be active and available for jobs in the specified category to run. If any resource or service is not available, the jobs in the specified category are temporarily suspended until the specified resource or service becomes available.

Typically, this script is used to define shared cluster resources for physical cluster nodes. For information about running this script in active/passive and active/active cluster environments, see the chapter on cluster support in the *AppManager Administrator Guide*.

This script is used to ensure that jobs do not run when required resources are not available. For example, you may want to check that the MSSQLServer and SQLExecutive services are running before running SQL script jobs. To do this, set the *Knowledge Script category* parameter to `sql` and the *Required active services* parameter to `MSSQLServer,SQLExecutive`.

If you are monitoring a cluster environment, you use this script to identify the cluster resources for the active physical node. For example, assume you have an active/passive Exchange cluster with two physical nodes, `SHASTA` and `VENICE` and that this cluster uses the logical drive `M:` as its shared cluster resource. This shared cluster resource is only available to the active physical node. You use this script to ensure that the Exchange Knowledge Script jobs only run on the active node by setting the *Knowledge Script category* parameter to `exch` and the *Required available resources* parameter to specify the `M:` drive.

To remove dependencies, you must cold start the AppManager Client Resource Monitor and AppManager Client Communication Manager services using the `-o` start parameter.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Knowledge Script job categories	Indicate the script category for which you want to specify resource dependencies. To specify multiple categories, separate the names with commas and no spaces. The default is all (*) job categories.
Required available resources (	Specify the physical resources required for running jobs in the specified category. Physical resources are file-system based and can include logical disk drives, directories, or specific files. You can enter multiple resources, separated by commas with no spaces. For example: `J:,K:,K:\temp\test.log`

Parameter	How to Set It
Required active services	Specify the Windows services required for running jobs in the specified category. Active services are services that are running when checked. To specify multiple services, separate service names with commas and no spaces: `MSSQLServer,SQLExecutive`
Raise event when update to required resources succeeds?	Select **y** to raise an event indicating the success of the operation. The default is n.
Event severity when update to required resources succeeds	Set the event notification level to give you the desired visibility for a successful operation. By default, the severity level is 25 (blue event indicator).

SiteSchedUpload

Use this Knowledge Script to specify a schedule for uploading data and/or events from the managed client's local repository on Windows to the current management server. You can set up specific schedules for data, events, or both, as needed.

Depending on your selection, the Client Communication Manager agent service (`NetIQCCM`) stores the events or data points in the local repository until the scheduled upload time. At upload time, the `NetIQCCM` service reads the events and/or data points from the local repository and sends them to the management server. The upload time starts when the job is scheduled to start and ends when the job is scheduled to stop, as specified on the Schedule tab.

The size of message batches delivered in the upload is configured through the ConfigSiteNetFlowCtrl Knowledge Script. You can also configure the maximum number of data points or events to store in the local repository with the SetLocalRPSize Knowledge Script.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**. However, you should use the Schedule tab to set a schedule appropriate to your environment.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Schedule upload time for data?	Select **y** to upload any data points stored on the managed computer to the central repository. The default is y.
Schedule upload time for events?	Select **y** to upload any events stored on the managed computer to the central repository. The default is n.
Raise event when attempt to set schedule succeeds?	Select **y** to raise an event indicating the success or failure of the operation. The default is n.
Event severity when attempt to set schedule...	Set the event severity level, from 1 to 40, to reflect the importance when the job: **... succeeds**. If you set this script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). **... fails**. The default is 5 (red event indicator).

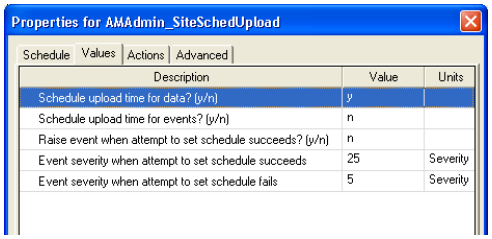
Example of How this Script Is Used

This script allows you to store performance and event data in the local repository until you are ready to upload it to the management server. By giving you the flexibility to transfer events and data during off-peak hours or when network traffic is light, the AppManager management server and repository can handle data from more servers and you can better manage network bandwidth.

For example, if you are collecting a significant amount of data on a few key managed clients, you may want to store the data locally on those managed clients while the network is busy, then transfer it to the management server at a time you know network traffic is light. In addition, you can schedule data from different managed clients to be uploaded at staggered times, further reducing the load on the management server and repository.

To use this script, set a schedule interval, start time, and end time on the **Schedule** properties tab. Click **Every** in the Frequency section to set an **End** time. The frequency interval (such as 5 Minutes) is ignored.

On the **Values** tab, you indicate whether this schedule applies to data, events, or both, and the event visibility. For example:



When you run this script on a target, the `NetIQccm` service immediately begins storing the specified information (in this case, data points) from all jobs running on the managed client in the managed client's local repository.

At the scheduled upload Start time (in this case, 1:00 a.m.), the information is transferred to the management server. If all the information in the local repository cannot be transferred to the management server, for example because the upload time is too short, any information not transferred remains in the local repository, up to the maximum number of events or data points that can be stored in the local repository. You can configure the maximum number of events or data points that can be stored in the local repository with SetLocalRPSize).

You can further control the flow of network traffic and the transfer of data from the managed client to the management server using the ConfigSiteNetFlowCtrl Knowledge Script.

UpgradeJobs

After you upgrade the AppManager agent, existing jobs on the managed client computer are not automatically upgraded to use the latest script functionality. Use this Knowledge Script to upgrade all child jobs for one or more parent jobs.

Note
The functionality provided in the latest version of the script may not be supported by older agents with older managed objects. For this reason, you should upgrade your managed clients to the latest version of the AppManager agent before you upgrade jobs running on those agents.

Upgrading jobs to use the latest script version allows the jobs to take advantage of the latest script logic while maintaining existing parameter values for the job, along with the associated graph data and event information. If the latest version of a script has been modified to have new parameters, for example, to create different events or data streams, the default values in the latest script for the new parameters are used.

This script upgrades all child jobs for one or more parent jobs. You can select the parent jobs you want to upgrade based on the following:

- **Knowledge Script** — Select this option to upgrade all ad hoc jobs started by the specified script. This option upgrades ad hoc jobs started by a particular script and ad hoc jobs started by a Knowledge Script Group member. This option does not upgrade policy-based jobs.
- **Knowledge Script category** — Select this option to upgrade all ad hoc jobs started by the specified script category. This option does not upgrade policy-based jobs.
- **Parent job identifier** — Select this option to upgrade all ad hoc child jobs that belong to the specified Parent Job ID. This option does not upgrade policy-based jobs.
- **Monitoring policy** — All policy-based jobs started by the specified Knowledge Script Group are upgraded. If you are using a Knowledge Script Group in one or more monitoring policies, all affected monitoring policies are updated. This option does not upgrade ad hoc jobs started by a Knowledge Script Group.

Note
This script does not upgrade AppManager report Knowledge Script jobs, nor does it return a list of report Knowledge Scripts in an instant check query.

Version Compatibility

This script upgrades the following:

- AppManager jobs on a version 6.0.2 (or later) Windows agent.
- Version 6.0 (or later) AppManager jobs on a version 7.0 (or later) UNIX agent.

Performing an Instant Check Query before Running this Knowledge Script

Before you attempt to upgrade jobs using this script, you should identify jobs that have not yet been upgraded by performing an **instant check query**.

The instant check query provides a list of jobs to upgrade and jobs that have already been upgraded. You should use the instant check query to identify the jobs to upgrade and to develop a strategy for upgrading existing jobs.

The instant check query identifies jobs by AppManager version and displays both Windows and UNIX jobs. Use the name of the script category to identify Windows or UNIX jobs.

The query results for each job also include the version of the AppManager agent. If the build version is:

- **6.0.x** - You have AppManager 6.0 or 6.0.2
- **7.0.x** - You have AppManager 7.0 (the latest version).

To perform an instant check query, use the **Instant Check Query** parameters on the Values tab. Use the *Select query* parameter to select the type of query you want. Then click **Browse (...)** in the *Display query* parameter to see the results of the selected query. To save the query results to a file, click **Finish**. You can run the following query types:

Query Type	Description
Out-of-date parent jobs	This query returns a list of parent IDs that you should upgrade. Note that some parent jobs may contain two different versions of a script. If that is the case, and either one of them is not the latest, the **KS Build ID** field reads "multiple build IDs."
Up-to-date parent jobs	This query returns a list of parent job IDs that are presently using the latest script in the repository and cannot be updated.
Old parent jobs with no upgrade	This query returns a list of jobs with an old script but for which there is no newer version in the repository. If this query returns any parent job IDs, it means the script has either been discontinued in later versions of AppManager, or it is a script you created or customized under a new name and for which you have yet to create a new version in the repository. When this query returns no values, then there are no parent jobs using out-of-date scripts. No further upgrading is required.
Child jobs on v6.x agents	This query returns a list of child jobs running on AppManager version 6.x agents.
Agent build IDs	This query returns a list of the agent build number on each computer. You can use this list to identify agents that you may want to upgrade.
Monitoring-policy jobs	This query returns a list of the jobs that are currently part of a monitoring policy. The jobs are listed according to the view or server group associated with the monitoring policy and then sorted by script group. Note that the Knowledge Script Group names (**KSGName** field) all have the prefix "KSG_." If you want to upgrade a Knowledge Script Group, add this prefix to the group name. You cannot upgrade any UNIX jobs that are policy-based. After you upgrade the backlevel UNIX agent to the latest version, remove the existing backlevel policy-based jobs and recreate them.

After you run an instant check query to identify the jobs you want to upgrade, you can generate a report that previews the jobs that would be upgraded. For more information, see "Viewing Job Upgrade Reports" on page 302.

Upgrading Jobs Created by a Custom Knowledge Script

If you have written a custom script, you do not need to upgrade existing jobs created by that script unless you have made changes to the script. In most cases, existing custom scripts can be run successfully on AppManager 7.0 (and later) agents.

Upgrading Jobs Created by a Copy of a Standard AppManager Knowledge Script

Before you can upgrade jobs created by a copy of a script, you must update the copy of the script in the AppManager repository:

To update a copy of a script:

1. On the repository computer, use Windows Explorer to open the `\netiq\appmanager\qdb\kp` folder and click the folder that contains the new version of the original script upon which the copy is based.
2. Copy the script and rename it to use the same name as the script copy.
3. Check the updated script copy into the repository. You are now ready to upgrade existing jobs.

Verifying Upgraded Jobs in the Operator Console

To verify that a job has been upgraded, view the job properties.

To verify a job upgrade:

1. In the List pane in the Operator Console, double-click a child job on the Jobs tab.
2. In the Properties dialog box, click **View KS**.
3. In the Script for Job dialog box, verify the **AppManID** is **Select 7.0**.

Resetting Password Information for Upgraded Jobs

In some rare cases, running the AMAdmin_UpgradeJobs script replaces the existing password for your environment with the default password specified in the original script properties. After these jobs are upgraded, they no longer run because the password is incorrect. This problem occurs for the following scripts:

- NTADMIN_AddUser
- NTADMIN_ChangePassword
- SQL_Bcp

If you upgrade any of these script jobs, update the job properties to restore the correct password information.

Resource Objects

Run this script on a managed Windows computer with the AppManager 6.0 (or later) agent where the "Log On As" account for the AppManager agent Client Resource Monitor (`NetIQmc`) service is a valid domain user account that belongs to the AppManager **Administrator** role.

To verify that the Windows user account that the AppManager agent uses belongs to the AppManager **Administrator** role, in AppManager Security Manager expand **AppManager Roles** in the TreeView and click **Administrator** to see a list of valid AppManager administrators.

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Instant Check Query	
Select query	The instant-check query provides a list of jobs to upgrade and jobs that have already been upgraded. You should use the instant check query to identify the jobs to upgrade and to develop a strategy for upgrading existing jobs. For more information, see "Performing an Instant Check Query before Running this Knowledge Script" on page 298.
Display query	Click **Browse [...]** to see a list of Knowledge Script jobs found by the instant check query.
Job Options	After you use *Instant check query* to identify the jobs you want to upgrade, use these parameters to generate a preview of the changes to the script that will be applied to existing jobs and to actually apply those changes and upgrade the jobs.
Upgrade jobs, or generate report?	Select one of the following options: • **Generate report** To preview detailed information about which jobs would be upgraded based on your selection criteria, select this option. If you select this option, no jobs are upgraded. This option provides detailed information about the changes to the actual script, including a list of new or changed parameters. If the latest script has new or changed parameters, you can preview the default values for these parameters before they are applied when you upgrade. • **Upgrade jobs** This option upgrades jobs based on your selection criteria. The default is Generate report. For more information, see "Viewing Job Upgrade Reports" on page 302.
Force, or restricted upgrade?	Select an option for upgrading parent jobs: • **Restricted** This option only upgrades a parent job if all of its child jobs are running on AppManager agents that have been upgraded to the latest version. If one of the child jobs for the specified parent job is running on an older agent, none of the child jobs are upgraded. • **Warning** When using the **Restricted** option, this script does **not** raise an event after unsuccessfully attempting to upgrade jobs on an older agent. Before you select this option, be sure to use the Instant Check Query to verify that there are no jobs running on older agents. • **Force** This option upgrades all of the child jobs for a parent, including child jobs that are running on an agent that has not been upgraded to the latest version. • **Warning** When using the **Force** option, this script does **not** raise an event after unsuccessfully attempting to upgrade jobs on a version 4.3 or 5.0 UNIX agent. If you are upgrading UNIX jobs, be sure to use the Instant Check Query to verify that there are no jobs on version 4.3 and 5.0 UNIX agents. Note that in some cases, the functionality provided in the latest version of the script logic may not be supported by older agents with older managed objects. The default is Restricted.

Parameter	How to Set It
Override job build version?	Set to **y** to upgrade jobs regardless of the job build version (force job upgrade). This option is required to upgrade jobs that have a build version that is the same or earlier than the script build version. The job upgrade process uses **all numbers** of the build version to compare versions. For example, if the build version for an AppManager job is **7.0.2** and the build version of the newer script is **7.0.112**, the job upgrade mechanism would **not** upgrade the job unless you enabled this option. The default is y. **Tip** To view the build version: • For a job, click the **View KS Script** button on the **Values** tab of the Job Properties dialog box. In the Script dialog box, the **AppManID** value specifies the build version. • For a script, in the Operator Console, right-click the script and click **Version History**. In the **Version** dialog box, the build version appears in the **Build ID** column.
Job selection criterion	Specify how to select the jobs you want to upgrade. You can select jobs by: • **Knowledge Script** Select this option to upgrade all ad hoc jobs started by the specified script. This option upgrades ad hoc jobs started by a particular script and ad hoc jobs started by a Knowledge Script Group member. This option does not upgrade policy-based jobs. • **Knowledge Script Category** Select this option to upgrade all ad hoc jobs started by the specified script category. This option does not upgrade policy-based jobs. • **Parent Job Identifier** Select this option to upgrade all ad hoc child jobs that belong to the specified parent job. This option does not upgrade policy-based jobs. • **Monitoring policy** All policy-based jobs started by the specified Knowledge Script Group are upgraded. This option does not upgrade ad hoc jobs started by a Knowledge Script Group. **Warning** If you are using a Knowledge Script Group in more than one monitoring policy, all affected monitoring policies are updated.
Job selection specification	Select the jobs you want to upgrade from a list, based on a job selection criterion. Click **Browse** (**...**) to see the list. If your job selection criterion is: • **Knowledge Script**, this list allows you to select the scripts you want to upgrade. This list only displays scripts that have a corresponding ad hoc job. • **Knowledge Script Category**, this list allows you to select the script categories you want to upgrade. This list only displays script categories that have a corresponding ad hoc job. • **Parent Job Identifier**, this list allows you to select one or more parent jobs. This list only displays parent job identifiers for ad hoc parent jobs. • **Monitoring policy**, this list allows you to select all policy-based jobs that belong to the specified Knowledge Script Group. This list only displays Knowledge Script Groups that belong to a monitoring policy. **Warning** If you are using a Knowledge Script Group in one or more monitoring policies, all monitoring policies are updated.

Viewing Job Upgrade Reports

Each time you run this script, job upgrade reports are created under:

`\netiq\temp\netiq_debug\`*`computer`*`\jobupgrade`

where *`computer`* is the name of the computer where you ran the report. The following reports are always generated regardless of whether you configure this job to generate a report or upgrade jobs:

- `Upgradejob_id.txt, where id` is the UpgradeJobs ID, provides information about which jobs are upgraded.
- `Upgradejob_id.rpt`, where *id* is the UpgradeJobs job ID, provides detailed information about each job.

Tip

`Upgradejob_id.log`, where *id* is the UpgradeJobs ID, lists the Job IDs that are upgraded and references the corresponding `.rpt` file and `.log` files for more information.

If the child of a specified parent job is running on an agent that has not been upgraded to the latest version, and you specified the **Restricted** upgrade option, the `UpgradeJob_<id>.txt` file displays information similar to the following:

```
Connected to SQL Server : RACKR14 repository QDB.
Time stamp: 03/03/07 14:20:47
  [Child Job] [Parent Job] [Build ID]  [Computer\KS]
2 4.3 agent(s) found.
2 5.0 agent(s) found.
1 5.0.1 agent(s) found.
Parent job 436 is skipped because under restricted mode, there cannot be any non-
7.0 agents.
Upgrade is finished.
Please check upgradejob_1343.rpt and upgradejob_1343.log located in
D:\NetIQ\Temp\NetIQ_Debug\RACKR14\jobupgrade.
Time stamp: 03/03/07 14:20:47
```

If the child of a specified parent job can be upgraded with parameter changes, the `UpgradeJob_<id>.rpt` file displays information similar to the following:

```
Connected to SQL Server : RACKR14 repository QDB.
Time stamp: 03/03/07 15:14:30
************************************************************
Parent job 54 can be upgraded under force mode.
2 4.3 agent(s) found.
2 5.0 agent(s) found.
2 5.0.1 agent(s) found.
1)
Child job ID = 55
Parent job ID = 54
KS name = NT_CpuLoaded
Machine name = RACKN08
Version = 4.6
Job 55 can be upgraded.
The following parameters in the existing job are not found in the new version of
the KS:
1) Event? (y/n)
Existing value is y.
2) Collect Data? (y/n)
Existing value is y.
3) Overall Load? (y/n)
Existing value is y.
4) Cpu Threshold >
Existing value is 0
5) Cpu Queue Length >
Existing value is 0
6) Event Severity
Existing value is 5
7) Severity for an unexpected KS error
Existing value is 35
The following parameters in the new version of the KS are not found in the
existing job:
1) Event Notification
Default value is NULL.
2) Create event if total system CPU is high?
Default value is y.
3) Severity - Total system CPU
Default value is 5
```

```
4) Create event if any individual CPU is high?
Default value is n.
5) Severity - Individual CPU
Default value is 15
6) Severity - Job failure
Default value is 35
7) Data Collection
Default value is NULL.
8) Collect total system utilization data?
Default value is y.
9) Collect individual processor utilization data?
Default value is n.
10) Collect processor queue data?
Default value is y.
11) Monitoring
Default value is NULL.
12) Threshold - Total system CPU
Default value is 0
13) Threshold - Individual CPU
Default value is 98
14) Threshold - Processor queue length
Default value is 0
Check for OldParameter tag
1) Create event if total system CPU is high?
Default value is y
OldParameter tag value = ?DO_EVENT="y" ((AND)) DO_OVERALL="y":"y":"n".
New StringValue = "y"
2) Severity - Total system CPU
Default value is 5
OldParameter tag value = ?DO_EVENT="y" ((AND))
DO_OVERALL="y":Severity:$default$.
New IntValue = "5"
3) Create event if any individual CPU is high?
Default value is n
OldParameter tag value = ?DO_EVENT="y" ((AND)) DO_OVERALL="n":"y":"n".
New StringValue = "n"
4) Severity - Individual CPU
Default value is 15
OldParameter tag value = ?DO_EVENT="y" ((AND))
DO_OVERALL="n":Severity:$default$.
No matching value, will keep original.
5) Severity - Job failure
Default value is 35
OldParameter tag value = PRM_KSERR.
New IntValue = "35"
6) Collect total system utilization data?
Default value is y
OldParameter tag value = ?DO_DATA="y" ((AND)) DO_OVERALL="y":"y":"n".
New StringValue = "y"
7) Collect individual processor utilization data?
Default value is n
OldParameter tag value = ?DO_DATA="y" ((AND)) DO_OVERALL="n":"y":"n".
New StringValue = "n"
8) Collect processor queue data?
Default value is y
OldParameter tag value = DO_DATA.
New StringValue = "y"
9) Threshold - Total system CPU
Default value is 0
OldParameter tag value = ?DO_OVERALL="y":TH_UTIL:$default$.
New IntValue = "0"
10) Threshold - Individual CPU
Default value is 98
OldParameter tag value = ?DO_OVERALL="n":TH_UTIL:$default$.
No matching value, will keep original.
11) Threshold - Processor queue length
Default value is 0
OldParameter tag value = TH_QLEN.
New IntValue = "0"
```

If the child of a specified parent job cannot be upgraded because the UNIX agent on which it is running is version 6.5, the entry looks like this:

```
Parent job 1536 cannot be upgraded under restricted mode.
29 6.5 agents are found.
Please upgrade these agents and restart the upgrade process.
```

In this case, upgrade the agent or use the *Force upgrade* parameter to upgrade the jobs on the older agent.

Chapter 6
AMAdminUNIX Knowledge Scripts

The AMAdminUNIX category contains Knowledge Scripts that perform administrative tasks for UNIX agents and your AppManager system. To run Knowledge Scripts in this category, you need to be defined as a user with administrator privileges. From within the Operator Console, you can select a Knowledge Script in the Knowledge Script pane and press **F1** for complete details.

Knowledge Script	What It Does
AgentHealthProxy	Checks the availability of a remote managed UNIX computer and monitors the health of the remote UNIX agent. This Knowledge Script uses a proxy UNIX agent to monitor remote UNIX agents.
AgentInstallProxy	Installs the AppManager UNIX agent on remote UNIX computers in your network. This Knowledge Script uses a proxy UNIX agent to install the UNIX agent on remote UNIX computers.
AgentUpdate	Updates the AppManager UNIX agent remotely on computers in your network.
AgentUpdateSecurityLevel	Updates the security level for the AppManager UNIX agent remotely on UNIX client computers in your network.
SchedMaint	Sets a server maintenance period for a managed computer. During the maintenance period, regularly scheduled AppManager jobs are prevented from running.
SetPrimaryMS	Sets the primary and secondary management server for UNIX agents in multiple management server configurations.

AgentHealthProxy

Run this Knowledge Script on an AppManager 7.0 (or later) UNIX agent to monitor the health of one more remote AppManager 7.0 (or later) UNIX agents.

When you drag this Knowledge Script to a computer in the TreeView, the Knowledge Script runs on that machine and tries to communicate with each of the remote computers in the machine list. This Knowledge Script:

- Checks the availability of a managed UNIX computer by first sending an ICMP Echo request to the managed UNIX computer. If the remote computer does not respond, this Knowledge Script sends an ICMP Echo request to the managed UNIX computer's default router and an event is raised.
- Monitors the health of the UNIX agent by checking a timestamp value created by the UNIX agent. Normally, the UNIX agent creates a timestamp value every 90 seconds. If the age of the timestamp value exceeds the threshold, an event is raised and the UNIX agent is restarted.
- This Knowledge Script enables self monitoring the UNIX agent health by raising appropriate events. You can use these events to correct unhealthy agents by restarting etc. This feature also enables you to restart unhealthy agents automatically without any manual intervention.

Use this Knowledge Script to remotely validate the health of the UNIX agent on a scheduled basis or for diagnostic purposes (for example, if there are gaps in data collection). This Knowledge Script is useful because it can detect a problem with a remote agent and reliably notify the AppManager administrator.

The proxy UNIX agent that runs the Knowledge Script must be configured to run as the **root** user account.

The remote UNIX agents you want to monitor, and the proxy UNIX agent that runs the Knowledge Script, must be Version 7.0 (or later). The remote UNIX agents must be accessible through the network from the computer where the proxy UNIX agent is installed. If you attempt to use this Knowledge Script to monitor a UNIX agent that is earlier than version 7.0, an event is raised that indicates "the timestamp is not found."

Do not use this Knowledge Script to monitor the health of the UNIX agent that runs the Knowledge Script. To successfully monitor the health of the proxy UNIX agent, run this Knowledge Script on another proxy UNIX agent.

To use this Knowledge Script to monitor more than one remote managed UNIX computer, all of the computers you want must be accessible using the same **root** user account information.

Note
Ensure that the nqmdaemon config file in the remote managed UNIX computers are not renamed to effectively monitor them.

This Knowledge Script can use either the Secure Shell (SSH) program with root password authentication or Telnet to make a secure connection to the remote UNIX or Linux computer. By default, SSH is used, but you can select **Telnet/FTP** from the **Connection Transport** list to use Telnet instead. If you choose to use Telnet, you must supply a non-root user account name and password.

Notes
Telnet and FTP send your username, password, and other information across the network in cleartext, making it easy for others to see this data.

If you are using Telnet to monitor the remote managed UNIX computer, ensure that su permission are given in the remote managed UNIX computer for that username.

Resource Objects

A managed UNIX computer where the AppManager 7.0 (or later) UNIX agent is installed. The UNIX agent must be configured to run as the **root** user account.

Default Schedule

The default interval for this script is **Every 10 minutes**.

To avoid raising false events, do not configure this Knowledge Script to run more frequently than the interval that the UNIX agent updates its timestamp. Ideally, the default interval should be more than 4 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Use the following parameters to raise events and set the severity level.	
Raise event if age of timestamp exceeds threshold?	Select the **Raise event** check box to raise an event if the the age of the timestamp exceeds the threshold limit set by you. By default, raising an event is enabled.
Threshold -- Maximum age of timestamp	Enter the maximum age of timestamp before an event is raised. The minimum threshold is 3 minutes and the maximum threshold is 99999 minutes. The default threshold is 9 minutes.
Event severity when age of timestamp exceeds threshold	If the age of the UNIX agent's timestamp value exceeds the specified threshold, set the event severity level, from 1 through 40, to indicate the importance of this event condition. The default severity is 8.
Remote Host Connection	
UNIX computers to monitor (comma-separated)	Enter the IP addresses of the remote UNIX computers you want to monitor, separated by commas and no spaces.
Password for root user account	Enter the root user account password that the proxy agent must use to connect to the remote UNIX computer. This is a mandatory field.
Connection Transport	Specify the connection mode between the proxy agent and the monitored UNIX computer: • **Telnet/FTP** to connect using Telnet. • **SSH/FTP** to connect using SSH.
Telnet non-root user account	Enter the Telnet non-root user account if you are using Telnet to connect to the monitored computer. Leave this parameter value blank if you are using SSH to connect to the monitored computer.
Telnet non-root user password	Enter the Telnet non-root user password if you are using Telnet to connect to the monitored computer. Leave this parameter value blank if you are using SSH to connect to the monitored computer.
Restart UNIX agent if age of timestamp exceeds threshold?	Select the **Restart Agent** check box to restart the UNIX agent if the age of the timestamp exceeds the threshold limit set by you. By default, restarting the UNIX agent is enabled.

Note

When running the AMADMINUNIX_AgentHealthProxy Knowledge Script with Secure Shell (SSH) as the connection method to the remote UNIX or Linux computer, if you specify an incorrect password for the root account, the Knowledge Script raises an event that incorrectly states that the login attempt was successful. If you see an event message similar to the event message below, you must update the job properties to specify the correct root password and start the job:

```
Output: Permission denied at /usr/netiq/UnixAgent/bin/UnixAgentHealthProxy.pl
More Info:
```

```
"SSH login OK to <machine> with root Using SSH/SFTP combination."
```

AgentInstallProxy

Use this Knowledge Script on a proxy UNIX agent to install the AppManager UNIX agent on remote UNIX and Linux computers in your AppManager site.

To successfully install the UNIX agent on a remote UNIX computer, the remote computer must be accessible through the network from the computer where the proxy UNIX agent is installed. This Knowledge Script can use either the Secure Shell (SSH) program with root password authentication or Telnet to make a secure connection to the remote UNIX or Linux computer. By default, Telnet is used, but you can select SSH/SFTP from the **Connection Transport** list to use Secure Shell instead. If you choose to use Telnet, you must supply a non-root user account name and password.

This Knowledge Script uses the UNIX agent as the proxy to install the AppManager agent on remote UNIX and Linux computers.

You should use this Knowledge Script if you want to:

- Install the AppManager agent for the first time on a remote UNIX or Linux computer.
- Perform a fresh installation of the agent, managed objects, and local repository on an existing managed client (for example, you do not want to preserve existing events, data, and jobs or want to use new information).

This Knowledge Script uses a silent installation file to specify how to install the UNIX agent and application monitoring support. If you have ever installed the agent on any host, a silent installation file is created on that host in `$nqmagt_home/log/silentinstall.ini`. The AgentInstallProxy Knowledge Script can use this file.

Or you can create a silent installation file. See "Sample Silent Installation File" on page 320 for an example. For complete information about creating a silent installation file, including information about configuring a silent installation file to install the UNIX agent with application-monitoring support, see "Performing a Silent Installation of the UNIX Agent" on page 316.

If you want to update the AppManager agent, currently installed managed objects, and the managed client's local repository, use the AgentUpdate Knowledge Script.

Note
To install the UNIX agent on a remote computer using a proxy running on Windows, a Knowledge Script in the AMAdmin category is available. For more information, see AMAdmin Knowledge Script help.

Running this Knowledge Script

The proxy UNIX agent where you run this Knowledge Script must be configured to run as the `root` user account.

All of the computers where you want to install the UNIX agent using this Knowledge Script must be accessible using the same root user account information.

The failure messages associated with a scenario where you inadvertently tried to run with an invalid root user account password may not clearly state this fact. If you see a failure that states, for example, "`Cannot switch to root user on [X computer]`," "`Permission denied at UnixAgentInstallProxy.pl line X`," "`unable to get a session to start the Installation`," or "`Unable to get a session to start the Installation for [X computer]`," first check to make sure you're using a valid root password.

If the .tar file or .ini file that you have specified for the "**Installation Source Configuration**" parameter (that is, the file that you intend to use for the installation on a remote computer) already exists in the directory you listed for the **Temporary directory on the remote computer** parameter, you'll see a failure. The event states, "`Can't FTP File <File Name>: permission denied`." If this occurs, just run the job again. After the initial failure, the .tar or .ini files will have been removed from the directory.

When you run this Knowledge Script using a hosts file, the hosts file should list any file locations of .ini files before it lists locations of .tar files. The job will fail and the Knowledge Script will transfer the .tar file and never transfer the .ini file unless you make sure to list the .ini files first.

Platform Support

This Knowledge Script supports all platforms supported by the UNIX agent, with the following exceptions:

- HP-UX in 32-bit and 64-bit mode is supported. Most AMAdminUNIX and UNIX Knowledge Scripts can run on HP-UX in 64-bit mode (because you can install and run the UNIX agent there). However, a computer running HP-UX in 64-bit mode cannot serve as a proxy.
- Red Hat Advanced Server (AS) 3.0 on Opteron with 64-bit operating system is supported with the UNIX agent running in 32-bit mode.
- Red Hat AS 3.0 on Itanium in 64-bit mode is supported.

Resource Objects

A managed UNIX computer where the AppManager 7.0 (or later) UNIX agent is installed. The UNIX agent must be configured to run as the root user account.

Default Schedule

By default, this Knowledge Script is **only run once on each proxy UNIX computer**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Set parameters for event notification.	
Raise event if installation fails?	Set to **y** to raise an event indicating that the installation has failed. By default, events are enabled.
Event severity when installation fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10 (red event indicator).
Raise event if installation succeeds?	Set to **y** to raise an event indicating that the installation is complete and has succeeded.The default is y.
Event severity when installation succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue event indicator).
Remote Host Connection	
Configure access to the remote managed computers by specifying their root password. All of the remote computers must use the same root password. This Knowledge Script can use SSH with root password authentication or Telnet to communicate with the remote managed computer.	

Description	How to Set It
Password for root user account	If you want to use Secure Shell (SSH) for the connection to the remote computers, make sure SSH with root authentication is enabled on the remote UNIX computers where you want to install the UNIX agent. For this parameter, you must specify the password for the root user to securely access the remote UNIX computers. This Knowledge Script does not support SSH root authentication with an RSA key.

Connection Transport	This Knowledge Script can use SSH with root password authentication or Telnet to communicate with the remote managed computer.
	If you select the Telnet/FTP option (the default), the Telnet prompt on the remote computer must end with a space or one of the following characters:
	`%`
	`>`
	`#`
	`$`
	Here is an example of a supported Telnet prompt:
	`user@hostname>`
	Here is an example of an unsupported Telnet prompt:
	`<user@hostname:/tmp - 2005-Mar-09>`
	`->`
	In the example above, the last character in the first line of the 2-line prompt is a line feed character, which is not supported.

Telnet non-root user account	If you selected Telnet to connect to the remote UNIX computers, specify a non-root user account to use for the connection. When connecting to a remote UNIX computer using Telnet and FTP, this Knowledge Script switches from the non-root user to the root user.
Telnet non-root user account password	If you selected Telnet as the connection transport medium, specify the password for the non-root user account to connect to the remote UNIX computers.

Installation Source Configuration

Set parameters to specify the remote computers where you want to install the UNIX agent, and the location of installation tar package and the silent installation file.

The simplest way to configure and run this Knowledge Script is to store the installation `.tar` packages and the silent installation files in the same directory, using the standard naming convention (see below). If these files are in the same directory and use the standard naming convention, you simply specify the remote UNIX computers where you want to install the UNIX agent and the directory where the installation files are located.

For installation `.tar` packages, the following naming convention applies:

- `UnixClient-aix.tar` for IBM AIX computers
- `UnixClient-hpux.tar` for HP-UX computers
- `UnixClient-linux.tar` for Red Hat and SuSe Linux computers
- `UnixClient-solaris.tar` for Sun Solaris computers

For silent installation files, the following naming convention applies:

- `UnixClient-aix.ini` for IBM AIX computers
- `UnixClient-hpux.ini` for HP-UX computers
- `UnixClient-linux.ini` for Red Hat and SuSe Linux computers
- `UnixClient-solaris.ini` for Sun Solaris computers
- `UnixClient - linux64` for Red Hat Linux on Itanium processors

If you do not use these standard names, you must specify the directory path and filename (see below).

Description	How to Set It
Full path to hosts file or list of computers where agent should be installed	Specify the computers you want by either: • Entering the full directory path and filename for the hosts file that contains a list of the remote managed UNIX computers where you want to install UNIX agents. For example, `/home/appmgr/agtinstalltarget`. This option enables you to configure different installation `.tar` packages and silent installation files for each computer. In the hosts file, list each hostname on a new line, for example: `labuws202::/agt/ua-usr.ini::/agt/UnixClient-linux.tar` where: `labuws202` is the name of the computer where you want to install the UNIX agent `/agt/ua-usr.ini` is the file path to the silent installation file `/agt/UnixClient-linux.tar` is the directory path to the agent installation package. The naming convention for the `.tar` files is explained in the help for the previous parameter. **Tips** To comment out a line in the hosts file, use a # character. The hosts file should list any file locations of `.tar` files before it lists locations of `.ini` files. See Running this Knowledge Script, above, for more information. • Specifying a comma-separated list of UNIX computers. If you use a list of computers instead of using a hosts file, you must also configure this Knowledge Script to specify the name and location of the silent installation file and the installation tar package. All the computers in the list must be installed using the same installation .tar package and silent installation file. This Knowledge Script attempts to install the agent on the first computer in the list. If an error occurs, or when the installation completes, the Knowledge Script attempts to install the agent on the next computer in the list. **Tip** To use this Knowledge Script to install the agent on multiple remote UNIX computers, all of the target computers must be using the same root password.
Installation without Hosts File	If you do not configure this Knowledge Script to use a hosts file, you must specify where the agent installation tar package and the silent installation file are located.
Directory path to agent installation .tar package(s)	If you have configured this Knowledge Script to use a hosts file, you do not need to configure this parameter. Enter the full path from the remote UNIX computer to the directory where the installation `.tar` package is located. For example: `/usr/local/agt` You do not need to specify the name of the installation tar package if the name of the installation tar package follows the naming convention. If the name of the file does not follow the naming convention, you must specify the path and filename.

Description	How to Set It
Name of silent installation file	If you have configured this Knowledge Script to use a hosts file, you do not need to configure this parameter. You do not need to configure this parameter if the name of the silent installation file follows the naming convention **and** the silent installation file is located in the same directory as the agent installation .tar package. If the name of the silent installation file does not follow the convention (but it is in the same directory as the installation package), enter the name of the silent installation file. If the silent installation file is not in the same directory as the installation `.tar` package, enter the directory path and name of the silent installation file. For example: `/usr/local/agt/UnixClient-Linux.ini`.
Installation Destination Specify a temporary directory on the remote computer to store a copy of installation files. Note that if UNIX agent communication is authenticated and encrypted (security level 2), this Knowledge Script does not copy the security key with the installation files. Make sure that the remote UNIX computer can access the key file according to the location specified in the silent installation file.	
Temporary directory on the remote computer	Specify the name of a temporary directory on the remote computer where you want to install the UNIX agent. This Knowledge Script copies the installation `tar` package and related files, such as the hosts file and the silent installation file to the temporary directory. Note that some operating systems have small `/tmp` directories, which can prevent this Knowledge Script from successfully copying the installation files and untarring the installation `.tar` package. For this reason, you can specify a directory other than `/tmp`. If the `.tar` file already exists in this directory, you'll see a failure the first time you run this Knowledge Script. See Running this Knowledge Script, above, for more information.
Installation command to run on the remote computer	Type the full command to use to install the UNIX agent on the target computer. The default is `UnixClient/netiq_agent_install.`

Performing a Silent Installation of the UNIX Agent

Performing a silent installation allows you to install AppManager UNIX agents and managed objects without interactively running the installation script. Like the silent installation of other AppManager components, the silent installation of the UNIX agent and UNIX managed objects uses an installation file that records the information required for completing the installation. Each line in the file is a *name*=*value* pair that provides the required information, for example, `HOME=/usr/netiq`.

You may want to manually create a silent installation file to install the UNIX agent, but if you have ever installed the agent on any host, a silent installation file that you can use is automatically created on that host in `$nqmagt_home/log/silentinstall.ini`.

Creating the Silent Installation File

The silent installation file consists of several required parameters in the form of *name*=*value* pairs with each parameter in a separate line.

The following parameters are required for silent installation.

Parameter	Description
AGREEMENT	Acceptance of the license agreement (y or n). For example: `AGREEMENT=y`
HOME	Installation home directory. For example: `HOME=/opt/netiq`

MS	The management servers with which the UNIX agent communicates, the port numbers on which they listen, the security level being applied to communications between the UNIX agent and the management server, and the location of the public encryption key file.
	This parameter allows you to specify multiple management servers across multiple repository databases.
	Here's an example of the syntax (all declarations need to be on a single line):
	`MS= { MS1 : Port # : Security Level : KeyFile ,`
	`MS2 : Port # : Security Level : KeyFile ,`
	`MS3 : Port # : Security Level : KeyFile ,`
	`MSn : Port # : Security Level : KeyFile }`
	Here is an example where 2 management servers are declared. The management server computers are `tc09k05` and `10.26.7.184`; the port where the management servers listen for communications from UNIX agents is 9001; the security level for UNIX agent communications is 2 (encryption and authentication); and the public key file is located in `/home/smba/keystore/key_1.pem`:
	`MS={tc09k05:9001:2:"/home/smba/keystore/key_1.pem",10.26.7.184:9001:2:"/home/smba/keystore/key_1.pem"}`

OWNER	Username that runs the UNIX agent. For example: `OWNER=root` If you specify a username other than `root`, you must also include the `NONROOT_EXTENSIONS` parameter.
NONROOT_EXTENSIONS	The non-`root` account for the UNIX agent to use the `sudo` program and the `sudoers` configuration file for root-level authority to access certain files or perform certain tasks. Allowing non-root extensions gives the UNIX agent account access to performance and application information that normally can only be accessed by the `root` super-user.
AUTOSTART	Automatic restart of the UNIX agent after installation (y or n). For example: `AUTOSTART=y`
AUTODISCOVERY	Perform automatic discovery of the UNIX computer resources after installation (y or n). For example: `AUTODISCOVERY=y`

Parameter	Description
MACHINENAME	Name of the UNIX computer to be displayed in the Operator Console TreeView. The name should be the full hostname for the computer and must be a name or address the management server can resolve for discovery to succeed. MACHINENAME=Full_host_name **Note** You can leave this parameter blank if AUTODISCOVERY is set to y to have the installation script attempt to resolve the hostname for you.
ADDITIONAL_STARTUP_OPTIONS	Any additional startup parameters you want the agent to use when it is restarted. Among those you may want to pass in are the -q 1 flag to enable Knowledge Script tracing, or the -C flag to cold-start the agent. After installation, these arguments appear in your nqmdaemon file. For information about agent startup options, see the *AppManager for UNIX Management Guide*.
INSTALL_PATCHES	Patch installation (y or n). Applicable only on Sun Solaris. Indicates whether to install operating-system patches that are included in the install package if they are needed. Hosts running Solaris 2.8 and 2.9 may require patches (109147 and 108434 for 2.8 and 111711 for 2.9) to make C++ runtime libraries available on the host. These patches do not require a system reboot and can be rolled back if necessary. Set this value to y to indicate that the patches should be automatically installed when needed. If the patches are needed and the parameter is not set, the Solaris installation will fail. The default is y.
DELETE_UNSUPPORTED_ APPLICATION_ MONITORING_MODULES	Indicates whether to continue the installation and delete any application monitoring modules (UNIX managed objects) that are currently installed but are no longer supported by the UNIX agent. The modules are obsolete and no longer supported by NetIQ. The installation prompt asks, “Do you wish to delete these modules and continue with the installation (y/n)?” The default is n.
DELETE_EXISTING_ APPLICATION_ MONITORING_MODULES	Indicates whether to continue the installation and delete any application monitoring modules (UNIX managed objects) that are currently installed. The UNIX agent upgrade deletes any previously installed application monitoring modules because they are not supported by the current version of the UNIX agent. These modules will be supported by the agent in the near future. The installation prompt asks, “Do you wish to delete the modules and continue with the installation (y/n)?” The default is n.

If you are upgrading from a previous release of AppManager, you need to include some additional parameters in the installation file. The following table summarizes these parameters:

Parameter	Description
BACKUPUA	Indicates how the backup copy of your previous UNIX agent installation should be handled. If you set this parameter to y, the backup copy of your old installation is saved in a new directory called $INSTALLPATH_<build_version> where <build_version> is the version of the agent from which you upgraded. If you set this parameter to n, the backup copy is deleted after the installation upgrade is verified. For example: BACKUPUA=n
INHERITCFG	Indicates how values should be set in your current UNIX agent configuration file. If you set this parameter to y, you do not need to specify many of the other parameters, such as the management server, because the values are inherited from your current configuration. However, you'll still need to include the following required parameters: AGREEMENT ADDITIONAL_STARTUP_OPTIONS AUTOSTART AUTODISCOVERY INSTALL_PATCHES DELETE_EXISTING_APPLICATION_MONITORING_MODULES DELETE_ UNSUPPORTED_APPLICATION_MONITORING_MODULES If you disable this parameter, you need to include all of the parameters in the installation file. For example: INHERITCFG=n If you set this parameter to n, any running jobs and their current configuration settings are **not** migrated, and the UNIX agent installation is treated as a new installation. All running jobs will no longer run. New jobs will have to be configured and started

Installing UNIX Managed Objects

If you are planning to install UNIX application monitoring modules using the silent installation file, you need to include additional parameters for those modules in the installation file.

For most UNIX applications, you must at least specify the managed object to install. For example, to install the DB2 and Apache managed objects, you would add the following parameters to the silent installation file:

```
apache=install
DB2=install
```

Note that the parameter is case-sensitive and must match the case and spelling of the application as defined in the .../UnixClient/mo/components file. For example:

Case Used for Parameter	Result
apache=install	Installs agent and application managed object correctly.
Apache=install	Installs agent but does not install application managed object.
APACHE=install	Installs agent but does not install application managed object.

Depending on the managed object you are installing, you may need to provide additional information in the installation file. For example, if you are installing the DB2 managed object you must also specify the DB2 instance name and, optionally, a valid DB2 username and password. Therefore, your silent installation file would also include the following parameters:

```
db2_instance=instancename
```

```
db2_user=johndoe
db2_password
```

A sample silent installation file is provided with each managed object in `$NQMAGT_HOME/mo/application_name/silent.cfg`. For example, for Tivoli Storage Manager (TSM) and a default UNIX agent installation directory, you would find the sample installation file in:

```
/usr/netiq/UnixAgent/mo/tsm/silent.cfg
```

For more information about any application-specific configuration, see the corresponding Management Guide in the `/Documentation` folder of the AppManager UNIX Components installation kit.

Executing the UNIX Silent Installation File

To install the UNIX agent according to the configuration specified in the silent installation file, you can execute the silent installation either from the command line or from a Knowledge Script. To execute the silent installation file from the command line, use the command-line option `-s` and the installation filename. For example:

```
./netiq_agent_install -s /tmp/silent.cfg.
```

Note
The installation filename must be specified as an absolute path.

To install the UNIX agent on remote UNIX and Linux computers, in addition to using this Knowledge Script, you can also use the AMAdmin_UnixAgentInstallProxy Knowledge Script, which uses the management server as the proxy to install the remote agent.

Sample Silent Installation File

A sample silent installation file is included with the UNIX agent tarball. When you untar the tarball, this file is saved in the root location where you performed the decompression. Use this file to create your own silent installation file, updating the parameters as needed.

For additional information on configuring the silent installation file to install application monitoring support, see "Performing a Silent Installation of the UNIX Agent" on page 316.

```
#####
#
# Sample NetIQ UNIX Agent (UA) Silent Installation File for
# the UNIX agent
#
#
#####
#
# The AGREEMENT directive declares whether you accept or
# decline the UA license agreement. An answer other than
# 'y' will stop the installation.
#
AGREEMENT=y
#
##
```

```
#
# The HOME directive declares the directory path where the
# agent should be installed. If you set this to a mount point
# (for example, "/usr"), the agent will be installed under
# (continuing the example) "/usr/netiq/UnixAgent".
# Otherwise, the agent will be installed under
# <your_path>/UnixAgent.
#
HOME=/usr/netiq
#
##
#
# The MS directive declares which management servers the UNIX
# agent should communicate with. It allows for support of
# multiple management servers across # multiple repositories.
# The first management server found for a given UNIX
# agent becomes the primary management server for that agent,
# the next one becomes the secondary (backup) management
# server, and so on. You can also specify a port number and
# security level for agent-to-management server
# communications. Supply all information on one line.
#
# The form of the MS directive is:
#
# MS= MS1 : Port # : Security Level : KeyFile ,
# MS2 : Port # : Security Level : KeyFile ,
# MS3 : Port # : Security Level : KeyFile ,
# MSn : Port # : Security Level : KeyFile
#
# Where:
#  "MS1" is the hostname or IP address of the management
#     server.
#  "Port" is the port number where the management server
#     listens for UNIX agent communications, typically 9001.
#  "Security Level" is 0, 1 or 2:
#     0: Cleartext messages
#     1: Encrypted communication only
#     2: Authentication and encrypted communication
#  "KeyFile" is the SSL key file.
#
# Examples:
#
# MS= {host1 : 9001 : 0 :"" , host2 : 9002 : 2 : /home/ keyfile1}
# MS= {10.26.7.184:9001 : 1 : "/home/smba/keystore/key_1.pem"}
# MS= {10.26.7.184:9001:2:"/home/smba/keystore/
```

```
#       key_1.pem",10.26.7.182:9001:0:""}
#
##
#
# The INHERITCFG directive determines whether to inherit the
# current UNIX agent configuration during upgrades, or to
# start with fresh values. Acceptable answers are 'y' and 'n'.
# This parameter only applies to reinstallations or upgrades.
#
INHERITCFG=y
#
##
#
# The BACKUPUA directive determines how to handle the backup
# copy of your previous UNIX agent installation. If you set
# this to y, the backup copy of your old UA installation is
# saved in a new directory, $INSTALLPATH_<build_version>,
# where <build_version> is the version of the agent from
# which you upgraded. If you set this parameter to n, the
# backup copy is deleted after the upgrade is verified.
# Acceptable values are 'y' and 'n'. This parameter only
# applies to reinstallations or upgrades.
#
BACKUPUA=y
#
##
#
# The OWNER directive supplies the user account that the
# UNIX agent should run under. Acceptable values include
# any valid user account on the target UNIX system.
#
##
#
OWNER=
#
##
#
# The NON_ROOT_EXTENSIONS directive declares whether to
# use sudo and other mechanisms (or extensions) to retrieve
# metrics normally accessible only by root users. If OWNER
# is non-root, NON_ROOT_EXTENSIONS must be set to "y".
#
NON_ROOT_EXTENSIONS=y
#
##
```

```
#
# ADDITIONAL_STARTUP_OPTIONS allow you to declare extra
# arguments to pass in to the UA process, 'nqmagt'. Among
# those you may want to pass in are '-q 1' to enable Knowledge
# Script tracing, or '-C' to cold-start the UNIX agent
# (clearing the local agent repository of jobs and data).
# After installation, these arguments appear in your
# nqmdaemon file.
#
ADDITIONAL_STARTUP_OPTIONS=
#
##
#
# The AUTOSTART directive declares whether to start the
# UNIX agent at the end of installation. Acceptable values
# are 'y' and 'n'. If you choose not to start the agent,
# you will need to do so later by running the nqmdaemon
# script. The recommended value is 'y'.
#
AUTOSTART=y
#
##
#
# The AUTODISCOVERY directive declares whether to try to
# automatically add an entry in the Operator Console TreeView
# for the UNIX agent and to discover it as part of the
# installation. Acceptable values are 'y' and 'n'. If the
# agent computer is already in the TreeView, selecting 'y'
# does not interfere with the current object. Recommended
# value is 'y'. If you set this to 'n', you must run the
# Discovery_UNIX Knowledge Script after the installation
# completes to discover the UNIX agent. If you set AUTOSTART
# to 'n', you must also set this parameter to 'n'.
#
AUTODISCOVERY=y
#
##
#
# The MACHINENAME directive declares the name that should be
# assigned to the UNIX agent computer once it has been added
# to the Operator Console TreeView or to Control Center. If
# AUTODISCOVERY is set to 'y', leave this parameter blank to
# have the installation script attempt to resolve the
# hostname for you.
#
```

```
MACHINENAME=
#
##
#
# The INSTALL_PATCHES directive declares that you want to
# install required operating system patches on Solaris. Hosts
# running Solaris 2.8 and 2.9 may require patches (109147
# and 108434 for Solaris 2.8, and 111711 for 2.9) to make
# C++ runtime libraries available on the host. These patches
# do not require a sytem reboot and can be rolled back if
# necessary. If the patches are needed and this directive is
# missing or set to 'n', the installation will fail.
# Acceptable responses are 'y' and 'n'.
#
INSTALL_PATCHES=n
#
##
#
# The DELETE_EXISTING_APPLICATION_MONITORING_MODULES
# directive declares whether to upgrade the UNIX agent if any
# currently installed application monitoring modules will be
# deleted as part of the upgrade. Acceptable values are 'y'
# and 'n'.
#
DELETE_EXISTING_APPLICATION_MONITORING_MODULES=n
#
#
# The DELETE_UNSUPPORTED_APPLICATION_MONITORING_MODULES
# directive declares whether to delete any application
# monitoring modules that are currently installed but are no
# longer supported by the version of the UNIX agent
# you're installing. Acceptable values are 'y' and 'n'.
#
DELETE_UNSUPPORTED_APPLICATION_MONITORING_MODULES=n
#
##
#EOF
```

AgentUpdate

Use this Knowledge Script to remotely update the AppManager UNIX agents in your network from an earlier version to the latest version. To use this Knowledge Script, the agent you want to update must run as **root**.

This Knowledge Script updates the AppManager UNIX agent and any application management files previously installed on the computer. For example, if you have a managed client that has an older version of the AppManager agent and AppManager for Apache management files, you can use this Knowledge Script to update the agent and the AppManager for Apache files on that computer.

If you run this Knowledge Script while existing Knowledge Script jobs are running, you must set the `INHERITCFG` flag in the silent installation file to `y` in order for the running jobs to continue. This flag specifies that the new version of the UNIX agent should keep the current configuration, which is specified within the `.ini` file you specify for the **Full path to silent configuration file** parameter (see below).

The topic titled "Creating the Silent Installation File" on page 316 discusses the `INHERITCFG` flag in the context of upgrading the UNIX agent.

With the default setting for `INHERITCFG` mentioned above, this Knowledge Script upgrades the target computer's local repository and migrates existing events, data, and jobs into the new local repository. Upgrading the local repository preserves any events, data, and jobs that are currently stored in the local repository. Jobs continue to use their current Knowledge Script properties after the upgrade. To start using any new Knowledge Script properties, start a new job after the update.

This Knowledge Script does **not** change the user account under which the UNIX agent runs. To change the agent's account, you must manually run the installation script on the managed client computer.

This Knowledge Script is configured by default to raise an event when:

- The agent update completes successfully. In this case, the following event message is displayed: "`Agent successfully upgraded to version` *`build_number`*."
- The agent update is in progress but was not completed within the expected 4-minute time period. In this case, the following event message is displayed: "`Agent upgrade started. Run this job again to check the status of the upgrade and clean up temporary files`." To verify that the agent update completed successfully, re-run this Knowledge Script on the managed UNIX client computer.

Note
This Knowledge Script updates only the objects previously installed on the managed client. If you want to install any new application management modules, run the appropriate installation script.

User Account Requirements for this Script

To run this Knowledge Script, the UNIX agent you want to upgrade must run as **root**. If the UNIX agent runs as a non-root user, you must run the interactive installation script on the local computer to upgrade the UNIX agent.

Resource Objects

Any UNIX computer where an earlier version of the AppManager agent has been installed.

Default Schedule

By default, this script is only run once for each computer.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if the update succeeds?	Set to `y` to raise an event indicating the upgrade was successful. If the upgrade fails for any reason, an event is generated regardless of how you set this parameter. The default is `y`.
Type of installation package (d for directory, t for tar file)	Type `d` if the installation files are uncompressed and located in a distribution directory. For example, type `d` if the installation files are located on a mounted CD drive or have been copied to a specific directory. Type `t` if the installation files are packaged in a tar file. The default is `d`. • If set to "`d`" for directory, the path you specify for the following parameter needs to point to the fully qualified path of the expanded tarball. • If set to "`t`" for tarball packaging, the path you specify for the following parameter needs to point to the fully qualified file name of the tarball, for example, `/home/appmanager/upgradefiles/UnixClient-aix.tar` for an AIX upgrade, where "`aix`" is the operating system on the target computer. **Note** Using the `tar` file requires additional scratch space in the temporary directory you specify on the target computer.
Full path to directory with UNIX agent .tar files	Enter the full path to the agent installation `.tar` file or the extracted contents of the `.tar` file. Typically the installation package is located on an accessible distribution computer. If you are working with the extracted contents of more than one `.tar` file, to avoid overwriting installation files you should extract each `.tar` file into its own shared directory. If the type of installation package is: • a `.tar` file, specify the full path to the `.tar` file. • extracted contents of the `.tar` file, specify the directory where the `netiq_agent_install` script is located.
Temporary working directory on the target computer	Specify a directory on the target computer to use as a temporary work space for upgrading the agent. Because the upgrade process creates a backup of your previous installation and verifies the success of the upgrade before removing any temporary files, the file system must have at least 200 MB of disk space available. The default is `/tmp`.
Full path to silent configuration file	Enter the full directory path to the silent installation file you'd like to use for the update. A full discussion of the silent installation file, including parameters and syntax, can be found in "Performing a Silent Installation of the UNIX Agent" on page 316. The default is `/tmp/silent.ini`.
Event severity when...	Set the event severity level, from 1 to 40, to indicate the importance of the event when the: • **... job aborts**. The default is 10 (red event indicator). • **... update fails**. The default is 10 (red event indicator). • **... update succeeds**. The default is 20 (blue event indicator).

AgentUpdateSecurityLevel

Use this Knowledge Script to remotely update the agent security level on the managed UNIX computers in your site. When configuring the security level for the agent, keep in mind that all managed UNIX clients in an AppManager site must be configured to use the same security level.

Use this Knowledge Script to change the security level on the managed UNIX clients in your AppManager site either before or after you change the security level on the repository database. The new security level takes effect on the managed UNIX client as soon as the Knowledge Script completes.

Keep in mind that managed UNIX clients cannot communicate with the management server until the security level on the managed UNIX client and the repository database are the same. After you restart the management server to use the latest security settings in the repository, managed UNIX clients with the corresponding security level can resume communication with the management server, and the Operator Console displays a success event message for this Knowledge Script job.

For more information about implementing AppManager secure communication, see the *Administrator Guide*.

The following security levels are available:

- **0 - Cleartext ~ no security** indicates that all communication between the agent and the management server is in cleartext and is not encrypted.
- **1 - Encryption ~ medium security** indicates that all communication between the agent and the management server is encrypted but the agent does not authenticate the identity of the management server.
- **2 - Encryption and authentication ~ highest security** indicates that the agent will attempt to authenticate the identity of the management server before sending and receiving encrypted communication. This option is only applicable if you installed the agent with **Encryption and Authentication**.

Tip If you configured the agent at installation to use **Cleartext** or **Encryption** and you want to change the security level to **Encryption and authentication**, you must reinstall the agent or manually change the agent's configuration file. See "Changing the Security Level for a UNIX Agent" in the *AppManager for UNIX Servers Management Guide* for more information.

Resource Objects

UNIX Server computers with the AppManager 6.0 (or later) agent.

Default Schedule

By default, this Knowledge Script is only run once for each computer.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if update succeeds or fails?	Set to y if you want AppManager to raise an event when the security level is successfully updated. This Knowledge Script always raises an event if the job does not run successfully. If enabled, you can configure the severity level of the event. The default is y.
Event severity when update...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **... succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **... fails**. The default is 5 (red event indicator).
Security level (0, 1, or 2)	Select the security level you want the managed UNIX computer to use: • **0 - Cleartext** if you want all communications between the agent and the management server to be in cleartext and is not encrypted. This option is best for closed network environments, testing, or troubleshooting communication issues. • **1 - Encryption** if you want all communications between the agent and the management server to be encrypted. • **2 - Encryption and authentication** if you want the management server to be authenticated before sending and receiving encrypted communication. Keep in mind that, for a single repository, all managed UNIX clients must use the same security level setting. Any time you update security, you must do so for all of your UNIX agents. If you cannot update all of your UNIX agents at once, the management server will not be able to communicate with those agents and the interruption in communication may result in missing critical events or data. Therefore, you should plan any change to the security level carefully to minimize the chance of communication failures. The default is 0 - Cleartext.

SchedMaint

Use this Knowledge Script to schedule a maintenance period for a specific application or for all resources on a managed client computer. During the maintenance period, regularly scheduled AppManager jobs do not run. You can specify the jobs you want to prevent from running by Knowledge Script category, or you can prevent all jobs from running on a server. For example, if you are planning routine maintenance on an Apache Server, you may want to block only the ApacheUNIX Knowledge Script jobs but if you are taking a computer offline to upgrade hardware or replace parts, you may want to prevent all jobs from running temporarily.

The maintenance icon  , indicates that a computer is in unscheduled maintenance mode (machine maintenance mode) or that all resources on a computer are in scheduled maintenance mode (that is, all jobs are blocked). When you see this icon, AppManager has temporarily stopped monitoring the computer.

You define the start and end time for the scheduled maintenance period on the **Schedule** tab when you set the job properties. Jobs resume running on the managed computer when the maintenance period expires.

Resource Object

Any UNIX computer

Default Schedule

By default, this script set to run **Daily** for a managed computer. However, you should use AppManager's scheduling capabilities found on the **Schedule** tab to set a schedule appropriate to your environment and maintenance needs. For more information about scheduling, see Example of How this Script Is Used.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Knowledge Script category to block	Enter the Knowledge Script category for the jobs you do not want to run during a maintenance period (for example, NetBackupUNIX to block only NetBackupUNIX Knowledge Script jobs). You must specify the full category name, but the name is not case-sensitive. You can specify either a single category or an asterisk (*) for all jobs on a target computer. The default is all jobs (*).
Raise event if schedule successfully implemented?	Set to **y** to raise an event indicating the success of the operation. The default is n.
Event severity when schedule...	Set the event severity level, from 1 to 40, to reflect the importance of each event. • **... successfully implemented**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful operation. The default is 25 (blue event indicator). • **... implementation fails**. The default is 5 (red event indicator).

Example of How this Script Is Used

In many environments, specific application servers have regularly scheduled periods when they are brought down by administrators so administrative tasks can be performed.

For example, an organization may have 20 Web servers that are shut once a month at 10 p.m. This interruption causes all of the AppManager jobs that are not explicitly stopped to error out and forces the administrator to restart the jobs manually when the servers are brought back online.

With this Knowledge Script, administrators can define a specific schedule for temporarily blocking jobs during a planned maintenance period.

Using the example above, you can use the **Schedule** tab to define a monthly schedule that blocks jobs on the last weekend of each month during a two-hour window.

Jobs that would normally run during this period, starting at 9:55 PM and ending at 11:55 PM are temporarily inactive. In this example, the actual maintenance period is short (just two hours once a month), but AppManager's scheduling capabilities provide enough flexibility for you to define a maintenance schedule that best meets your needs.

On the **Values** tab, you can identify a specific Knowledge Script category to block such as ApacheUNIX or you can use the default (*) to block all of the jobs if the computers are going to be physically shut down. For example, to block all of the UNIX Knowledge Script jobs you might set the **Knowledge Script category to block** parameter to `Unix`.

At 9:55 PM local time (on the computer where the job is running), the maintenance period begins and all UNIX Knowledge Script jobs running on the target computers become inactive to allow for the scheduled maintenance. At 11:55 local time, the maintenance period expires and the jobs resume running at their regularly scheduled intervals.

SetPrimaryMS

Use this Knowledge Script to set or change the primary or secondary management server for UNIX agents, or to change the port number of the primary or secondary management server.

This Knowledge Script allows you to explicitly designate a primary and a secondary management server and therefore explicitly control the communication between the managed UNIX clients and the management servers authorized to communicate with those managed clients. This Knowledge Script allows you to specifically assign a single primary management server for specified UNIX agents. Once you have identified a primary management server, the UNIX agent sends all information to that computer.

To help ensure communication is maintained even if the primary management server goes down, you can also use this Knowledge Script to explicitly designate a secondary or backup management server for the managed client. If the primary management server for the managed client fails, the backup management server will take over communication with the managed client until communication with the primary management server is restored.

If the target UNIX agent computer does not have the specified management server defined in its configuration file (`NqmComms.xml`), the agent adds it to the configuration file and then sets the flags according to the value you've set for the **Select the management server operation to perform** parameter.

If you run the job from a management server computer, be aware that the job can only set a primary or backup management server when the specified management server is associated with the same repository. For example, Management Server A for Repository 1 cannot specify that Management Server B for Repository 2 should now become the primary or backup management server for Repository 1.

Notes

When you install the UNIX agent, you implicitly establish a primary management server and can use this Knowledge Script to change the primary management server or designate a secondary management server. We recommend, however, that you explicitly designate the primary and secondary management servers by running this Knowledge Script twice.

The first time you run the job, you should identify the primary management server. After you receive notification that setting the management server has been successful, you can run the script a second time to set the secondary management server. You can also use this Knowledge Script to remove a management server for a target UNIX agent.

Resource Object

UNIX computer icon

Default Schedule

By default, this script is **only run once for each computer**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if job succeeds or fails?	Set to **y** to raise events that indicate whether the management server configuration succeeded or failed. By default, events are enabled. If this parameter is enabled and the management server is configured successfully for the UNIX agent, an informational event is raised (blue event indicator). If the configuration of the management server fails, a severe event is raised (red event indicator).
Management server hostname or IP address	Enter the name or IP address of the management server you want to set as a primary or secondary management server or that you want to remove for a UNIX agent. Keep in mind that you should set the primary management server first, then rerun this script to set the secondary management server or to make any changes to either the primary or secondary management server. **Note** Although you can specify the management server by hostname or IP address, based on how you have your site configured, the event detail message always identifies the computer by IP address.
Management server operation to perform	Select the appropriate option for the management server you have specified. • **Set primary management server** to change the primary management server • **Set secondary management server** to change the backup management server • **Unset management server** to remove the specified management server as a valid management server for the target computer **Note** If the target computer does not have the specified management server defined in its configuration file (`NqmComms.xml`), the UNIX agent adds it to the configuration file and then sets the flags according to the value you've set here. The default is Set primary.
Port number for the management server	Type the port number you want to use on the management server for communications from UNIX agents. The port number should be the same port you specified when you installed the management server or the port number you have set for the `UNIX port` in the management server registry. **Note** If you have changed the port number for UNIX agents in the management server registry, run this script to set the new port number on your UNIX agents, then restart the management server to restore communication. The default is port number `9001`.
Event severity when job succeeds or fails	Set the event severity level, from 1 to 40, to indicate the importance of the event when setting the management server fails. The default severity level is 5 (red event indicator).

Example of How this Script Is Used

When you establish a **primary management server** for a managed client, that management server becomes the only management server that the managed client communicates with for a single repository/management server configuration. A **secondary** or **backup management server** can also be defined for each managed client in case the primary management server fails. The secondary management server only communicates with the managed client when the primary management server is unavailable. When communication with the primary management server resumes, the managed client resumes exclusive communication with the primary management server.

Because a multiple management server environment is chiefly intended for failover functionality (to provide an alternative management server if the primary management server fails), each managed client can have one primary management server and one backup management server for each repository.

Chapter 7
AM Health Knowledge Scripts

The AppManager Self Monitoring module, also known as AM Health, provides Knowledge Scripts for monitoring the health and availability of AppManager components. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
CCComponentsHealth	Monitors the health and availability of SQL Server resources associated with Control Center components.
HeartbeatUNIX	Monitors the AppManager agent heartbeat in a UNIX environment.
HeartbeatWin	Monitors the AppManager agent heartbeat in a Microsoft Windows environment.
QDBComponentsHealth	Monitors the health and availability of SQL Server resources associated with the AppManager repository (QDB) and the Management Server.
Recommended Knowledge Script Groups	Perform essential monitoring of AppManager components.

CCComponentsHealth

Use this Knowledge Script to monitor the health and availability of Microsoft SQL Server resources associated with AppManager Control Center components. These components include the Cache Manager, Command Queue Service, Deployment services, and Control Center repository (`NQCCDB`).

This script monitors the percentage of database space and log space used, the amount of time required for a SQL command or query to execute, and the status of AppManager scheduled tasks, which are SQL Server agent jobs operating on the AppManager repository (`QDB`). This script can restart a service or job that is down.

This script raises events for the following situations:

- SQL Server services are down, restarted, or missing
- The Command Queue Service (CQS) is down or is not connected to the Control Center repository
- Control Center Cache Manager errors occur
- Queries take too long to process
- Deployment services are down
- Database or log space is low

Resource Objects

- Cache Manager
- Command Queue Service
- Deployment services
- Control Center repository

Default Schedule

The default interval for this script is every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise an event if SQL Server services are down?	Select **Yes** to raise an event if Control Center SQL Server services are down. The default is Yes. **Tip** Use Action Script for notification, as the Control Center repository will not be available.
Event severity when SQL Server services are down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which SQL Server services are down. The default is 5.
Restart SQL Server services that stop unexpectedly?	Select **Yes** to restart SQL Server services that stop unexpectedly, such as when not as part of scheduled maintenance. The default is Yes.

Parameter	How to Set It
Raise an event if SQL Server services cannot be restarted?	Select **Yes** to raise an event if SQL Server services cannot be restarted. The default is Yes. **Tip** Use Action Script for notification, as the Control Center repository will not be available.
Event severity when SQL Server services cannot be restarted	Set the event severity, from 1 to 40, to indicate the importance of an event in which SQL Server services cannot be restarted. The default is 5.
Raise an event if SQL Server services are restarted?	Select **Yes** to raise an event if SQL Server services are successfully restarted. The default is Yes.
Event severity when SQL Server services are restarted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which SQL Server services are successfully restarted. The default is 30.
Raise an event if Control Center Cache Manager errors occur?	Select **Yes** to raise an event if Cache Manager experiences errors related to Microsoft Distributed Transaction Control (MSDTC). The default is Yes. When this parameter is enabled, AppManager raises events if MSDTC is configured improperly or is unavailable. Cache Manager is a child process of the CQS. Cache Manager runs the Control Center queries on AppManager repository computers to retrieve view information for a Control Center management group.
Event severity when Cache Manager errors occur	Set the event severity, from 1 to 40, to indicate the importance of an event in which Cache Manager experiences errors. The default is 10.
Raise an event if Control Center SQL Server jobs are missing?	Select **Yes** to raise an event if SQL Server jobs are missing. The default is Yes. A missing job is one that may have been deleted or renamed.
Event severity when Control Center SQL Server jobs are missing	Set the event severity, from 1 to 40, to indicate the importance of an event in which SQL Server jobs are missing. The default is 15.
Raise an event if Control Center SQL Server jobs are disabled?	Select **Yes** to raise an event if SQL Server jobs are disabled. The default is Yes.
Event severity when Control Center SQL Server jobs are disabled	Set the event severity, from 1 to 40, to indicate the importance of an event in which SQL Server jobs are disabled. The default is 15.
Enable SQL Server jobs that are disabled?	Select **Yes** to enable, or start, SQL Server jobs that are disabled. The default is Yes.
Event severity when SQL Server jobs cannot be enabled	Set the event severity, from 1 to 40, to indicate the importance of an event in which disabled SQL Server jobs cannot be enabled, or started. The default is 15.
Raise an event if SQL Server jobs are successfully enabled?	Select **Yes** to raise an event if disabled SQL Server jobs are successfully enabled, or started. The default is unselected.
Event severity when SQL Server jobs are successfully enabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which disabled SQL Server jobs are successfully enabled, or started. The default is 20.
Raise an event if a Control Center SQL Server job fails?	Select **Yes** to raise an event if any step in a SQL Server job fails. The default is Yes.
Event severity when a Control Center SQL Server job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a SQL Server job fails. The default is 20.
Raise an event if Control Center server disks are fragmented?	Select **Yes** to raise an event if disks on the Control Center server are fragmented. The default is Yes. **Tip** To avoid errors when running this script on a Windows Server 2008 server, disable User Account Control (UAC).

Parameter	How to Set It
Event severity when disks are fragmented	Set the event severity level, from 1 to 40, to indicate the importance of an event in which disk fragmentation has occurred on the Control Center server. The default is 15.
Raise an event if query process time exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to process a SQL query exceeds the threshold you set. The default is Yes.
Threshold -- Maximum process run time	Specify the maximum length of time it can take SQL Server processes to run before an event is raised. The default is 300 seconds.
Event severity when query process time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which SQL query processing time exceeds the threshold you set. The default is 5.
Event severity when query process time cannot be retrieved	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the script cannot determine the processing time for SQL queries. Processing time could be prevented from being retrieved if the query fails due to blocking, or if a connection cannot be made to the Control Center QDB SQL Server, which would cause the query to fail. If the query fails, the event will be raised without exception, which would inform users if there was an issue with the Control Center QDB SQL Server. The default is 10.
Raise an event if Deployment services are down?	Select **Yes to** raise an event if Control Center Deployment services are down. The default is Yes. The following situations can cause Deployment services to be down: • The Control Center server is restarted. • Deployment services took too long to restart. • The connection to the Control Center repository is unavailable. • The proxy server is unavailable.
Event severity when Deployment services are down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Deployment services are down. The default is 15.
Raise an event if unable to retrieve Control Center component information?	Select **Yes** to raise an event if the script does not have the discovery details for the Control Center components, or if the discovery details are empty. The default is Yes.
Event severity when unable to retrieve Control Center component information	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot retrieve Control Center Component information. The default is 10.
NetIQ Control Center Command Queue Service Monitoring	
Raise an event if Command Queue Service is not connected to the Control Center database?	Select **Yes** to raise an event if the Command Queue Service (CQS) is not connected to the Control Center database (`NQCCDB`). The default is Yes. The CQS polls the Command Queue table for queries to run. The Command Queue table stores queries that collect view information based on the criteria defined in Control Center.
Event severity when Command Queue Service is not connected to the Control Center database	Set the event severity, from 1 to 40, to indicate the importance of an event in which the CQS is not connected to the Control Center database (`NQCCDB`). The default is 5.
Raise an event if Command Queue Service is down?	Select **Yes** to raise an event if the CQS is down. The default is Yes.
Event severity when Command Queue Service is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CQS is down. The default is 15.
Restart Command Queue Service if the service is down?	Select **Yes** to restart CQS if it is down. The default is Yes.

Parameter	How to Set It
Raise an event if Command Queue Service is restarted?	Select **Yes** to raise an event if CQS is successfully restarted. The default is Yes.
Event severity when Command Queue Service is restarted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CQS is successfully restarted. The default is 15.
Raise an event if Command Queue Service cannot be restarted?	Select **Yes** to raise an event if CQS cannot be restarted. The default is Yes.
Event severity when Command Queue Service cannot be restarted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CQS cannot be restarted. The default is 15.
Data Collection	
Collect data for database space utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of database space used on the Control Center server. The default is unselected.
Collect data for log space utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of log space used on the Control Center server. The default is unselected.
Collect data for Command Queue Server connection status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns **100** if CQS is up and **0** if CQS is down. The default is unselected.
Collect data for SQL Server service status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns **100** if SQL Server services are up and **0** if SQL Server services are down. The default is unselected.
Monitoring	
SQL username	Specify the username required to access SQL Server on the Control Center server.
SQL Server File Size and Growth Settings Monitoring	
Raise an event if insufficient space available for further file growth?	Select **Yes** to raise an event if the amount of available disk space is not enough to allow the file to continue to grow. SQL Server has growth settings on the Database Data and Log files. If the amount of free space on the disk is lower than this growth setting, an event will be raised to keep the files from attempting to grow and causing the SQL Server to terminate. The default is Yes.
Event severity when available space is insufficient	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the available server space is insufficient. The default is 10.
Raise an event if file growth rate falls below the threshold?	Select **Yes** to raise an event if the growth rate of the database data and log files falls below the threshold you set. If the growth rate is low, the data and log files become fragmented, which negatively impacts performance. **Note** The two threshold parameters (MB and percentage) are evaluated individually. The default is Yes.
Threshold -- Minimum growth rate in MB	Specify in megabytes the minimum growth rate of SQL Server files before an event is raised. The default is 256 MB.
Threshold -- Minimum growth rate in percentage	Specify as a percentage the minimum growth rate of SQL Server files before an event is raised. The default is 9%.
Event severity when file growth rate falls below the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the rate of growth of SQL Server files falls below the threshold you set. The default is 10.

Parameter	How to Set It
Raise an event if SQL maximum file size exceeds disk space?	Select **Yes** to raise an event if the maximum SQL file size (`MAXSIZE`) is set to a value greater than the amount of available disk space. The default is Yes. The `MAXSIZE` value identifies the maximum size to which a SQL Server database can grow.
Event severity when SQL maximum file size exceeds disk space	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the maximum SQL file size is set to a value greater than the amount of available disk space. The default is 15.
Raise an event if Autogrowth is not enabled and file usage exceeds the threshold?	Select **Yes** to raise an event if the file usage exceeds the threshold and Autogrowth is not enabled. The default is Yes. The Autogrowth feature allows a database to grow by the amount of space required by a file or a transaction.
Threshold -- Maximum file usage with Autogrowth disabled	Specify the maximum amount of file usage with Autogrowth disabled that can occur before an event is raised. The default is 90%.
Event severity when Autogrowth disabled and usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the file usage exceeds the threshold and Autogrowth is not enabled. The default is 10.
Event severity for a Knowledge Script error	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this Knowledge Script job fails. The default is 10.

HeartbeatUNIX

Use this Knowledge Script to test the heartbeat of the AppManager agent computer running UNIX. A heartbeat is a periodic signal generated by an AppManager agent computer to indicate that it is still running.

You can set this script to raise an event for the following conditions:

- Heartbeat fails
- An agent is healthy, such as when the heartbeat returns after failing
- The agent heartbeat fails a user-specified number of times

Note
If you use this Knowledge Script with the AppManager Operator Console, you can access the Actions and Advanced tab, but the options on those two tabs will not function.

Resource Objects

UNIX servers

Default Schedule

The default interval for this script is every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Heartbeat Options	
Raise an event if the agent heartbeat fails?	Select **Yes** to raise an event if the heartbeat for the AppManager agent server stops. The default is Yes.
Event severity when the agent heartbeat fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the heartbeat stops. The default is 5.
Raise an event when agent heartbeat restarts?	Select **Yes** to raise an event if the heartbeat starts again after stopping. The default is Yes.
Event severity when the agent heartbeat restarts	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the heartbeat starts again after stopping. The default is 25.
Number of consecutive heartbeat failures before raising an event	Specify the number of times the heartbeat must fail before raising an event. The default is 1.
Generate heartbeat data?	Select **Yes** to enable the heartbeat check. If you select Yes and the data point from this job is missing, AppManager raises an event. If you select No, the heartbeat check will not look for the data point from this job. The default is Yes.
Heartbeat Investigation Steps (Used by Management Server)	AppManager performs the following steps only if the heartbeat event or the heartbeat data is missing.

Parameter	How to Set It
Attempt to contact agent computer by ICMP ping?	Select **Yes** to send an ICMP ping request to the agent computer. The default is Yes.
Perform tracert diagnostic if ICMP ping fails?	Select **Yes** to run a tracert (traceroute) diagnostic test if the ping request fails. The default is Yes. A traceroute test helps you troubleshoot network routing problems that can block ICMP traffic. This script raises an event if the tracert fails.

HeartbeatWin

Use this Knowledge Script to test the heartbeat of the AppManager agent computer. A heartbeat is a periodic signal generated by an AppManager agent computer to indicate that it is still running.

This script raises events if the heartbeat for the agent computer stops or restarts, and it generates a data point about the heartbeat events. You can also use this script to track whether jobs finish in the expected time frame, or if they exceed the maximum run time.

You can set this script to raise an event for the following conditions:

- Heartbeat fails
- An agent is healthy, such as when the heartbeat returns after failing
- The agent heartbeat fails a user-specified number of times
- Jobs take longer than expected to execute
- Jobs exceed maximum run time
- No jobs are found

Note
If you use this Knowledge Script with the AppManager Operator Console, you can access the Actions and Advanced tab, but the options on those two tabs will not function.

Resource Objects

Windows servers

Default Schedule

The default interval for this script is every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Heartbeat Options	
Raise an event if the agent heartbeat fails?	Select **Yes** to raise an event if the heartbeat for the AppManager agent server stops. The default is Yes.
Event severity when the agent heartbeat fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the heartbeat for the AppManager agent server stops. The default is 5.
Raise an event when agent heartbeat restarts?	Select **Yes** to raise an event if the heartbeat starts again after stopping. The default is Yes.
Event severity when the agent heartbeat restarts	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the heartbeat starts again after stopping. The default is 25.
Number of consecutive heartbeat failures before raising an event	Specify the number of times the heartbeat must fail before raising an event. The default is 1.
Generate heartbeat data?	Select **Yes** to enable the heartbeat check. If you select Yes and the data point from this job is missing, AppManager raises an event. If you select No, the heartbeat check will not look for the data point from this job. The default is Yes.

Parameter	How to Set It
Job Monitoring Options	
Monitor individual jobs?	Select **Yes** to monitor *all* jobs running on the agent that came from the same QDB as the heartbeat job. If you select No, the heartbeat job simply sends the heartbeat event and data according to the heartbeat-related parameters you set for this Knowledge Script. The default is Yes.
Raise an event if jobs take longer than average to execute?	Select **Yes** to raise an event that lists all jobs that are taking longer to execute than their average execution time. The agent stores a list of the average times jobs take to execute. The default is Yes.
Ignore jobs running for less than this amount of time	If you want to ignore jobs that are running for certain length of time, specify the running time for jobs that will be ignored. The default is 30 seconds.
Grace period	Specify a number to represent the grace period for job execution. The grace period is a multiple of the average time a job takes to execute. The agent stores a list of the average times jobs take to execute. For example, if you specified a grace period of 5, this script would take that value and multiply it by the average time a job takes to execute. If a job took one second to execute on average, the grace period would be 5 seconds. If the job takes longer than 5 seconds, the script raises an event. The default grace period is 5.
Event severity when jobs take longer than average to execute	Specify the event severity, from 1 to 40, to indicate the importance of an event in which the execution time for Knowledge Script jobs is longer than the average execution time for that job. The default is 5.
Raise an event if jobs take longer than their schedule to execute?	Select **Yes** to raise an event that lists all jobs that are taking longer to execute than their scheduled time to execute. The scheduled time is how often the job is set to run, such as every five minutes. The default is Yes.
Event severity when jobs take longer than their schedule to execute	Specify the event severity, from 1 to 40, to indicate the importance of an event in which the execution time for a Knowledge Script job is longer than the script's schedule. The default is 5.
Raise an event if job exceeds maximum job run time?	Select **Yes** to raise an event if the run time for a Knowledge Script job exceeds the *Maximum job run time* threshold. The default is Yes.
List of Knowledge Scripts to skip "Maximum job run time" check	Provide a comma-separated list of the Knowledge Scripts that you do not want to compare to the *Maximum job run time* threshold.
Maximum job run time	Specify the maximum number of seconds a Knowledge Script job can run before an event is raised. The default is 180 seconds.
Event severity when job exceeds maximum job run time	Set the event severity, from 1 to 40, to indicate the importance of an event in which the run time for a Knowledge Script job exceeds the *Maximum job run time* threshold. The default is 5.
Raise an event if no jobs found?	Select **Yes** to raise an event if no Knowledge Script jobs are running. The default is unselected.
Event severity when no jobs found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no Knowledge Script jobs are running. The default is 35.
Timeout when processing jobs	Specify how long AppManager should wait for the agent to process jobs before assuming the agent either will not respond or has timed out. Use this parameter to monitor agents that are consistently taking longer than expected to respond. If the agent doesn't respond before your specified timeout value, AppManager raises an event stating that it was unable to process this command and suggesting you increase the timeout value. The event might also include data about a Windows error, if one was generated. The default timeout is 10 seconds.

Parameter	How to Set It
Use XML formatting in event message?	Select **Yes** to format event messages in XML. The default is Yes. Leave this parameter unselected to format event detail messages in plain text. Events formatted in XML display results in tables. Events in plain text display results in rows of unformatted text.
Knowledge Script Options	
Event severity when unexpected error occurs	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this Knowledge Script job fails or any other unexpected event occurs. The default is 35.
Heartbeat Investigation Steps (Used by Management Server)	AppManager performs the following steps only if the heartbeat event or the heartbeat data is missing.
Attempt to contact agent computer by ICMP ping?	Select **Yes** to send an ICMP ping request to the agent computer. The default is Yes.
Perform tracert diagnostic if ICMP ping fails?	Select **Yes** to run a tracert (traceroute) diagnostic test if the ping request fails. The default is Yes. A traceroute test helps you troubleshoot network routing problems that can block ICMP traffic. This script raises an event if the tracert fails.
Connect to agent NetIQmc port if ICMP ping succeeds?	Select **Yes** to attempt a connection to the `NetIQmc` port on the agent computer. The default is Yes. The connection is attempted only if the ping attempt succeeds. This script raises an event if the ping fails.
Use RPC to probe agent if port check succeeds?	Select **Yes** to send a Remote Procedure Call (RPC) to the agent computer. The default is Yes. The RPC is sent only if the port connection succeeds. This script raises an event if the RPC probe fails.
Test agent computer registry if RPC probe succeeds?	Select **Yes** to allow the management server to attempt to use the Remote Registry Service to connect to the Windows Registry on the agent computer. The connection is attempted only if the RPC probe succeeds. The management server must have sufficient privileges to connect to the Registry. The default is unselected. This script raises an event if the management server cannot connect to the Registry.
Check status of agent services if registry test succeeds?	Select **Yes** to allow the management server to verify whether the NetIQ agent services, `NetIQccm` and `NetIQmc`, are running. This test is attempted only if the registry test succeeds. The management server must have sufficient privileges to access the agent services. The default is unselected. This script raises an event if the agent services are up or down.

QDBComponentsHealth

Use this Knowledge Script to monitor the health of NetIQ AppManager repository (QDB) and Management Server components.

This script monitors SQL Server resources associated with the QDB, including the percentage of database space and log space used, the time taken for a SQL command or query to execute, and the status of AppManager scheduled tasks. If a service or job is down, this script can restart it.

You can set this script to raise an event for the following conditions:

- Any SQL Server services are down or missing
- Database or log space is low
- The Management Server isn't connected
- The Management Server service is down
- Queries are taking too long to process.

Resource Objects

Windows servers

Default Schedule

The default interval for this script is every thirty minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise an event if SQL Server services are down?	Select **Yes** to raise an event if SQL Server services are down. The default is Yes. **Tip** Use Action Script for notification, as the Control Center repository will not be available.
Event severity when a SQL Server service is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a SQL Server service is down. The default is 5.
Restart SQL Server services if the services are stopped unexpectedly?	Select **Yes** to restart the SQL Server services if the services stop unexpectedly. The default is Yes.
Raise an event if a SQL Server service restart fails?	Select **Yes** to raise an event if a SQL Server service fails to restart. The default is Yes. **Tip** Use Action Script for notification, as the Control Center repository will not be available.
Event severity if a SQL Server service fails to restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a SQL Server service fails to restart. The default is 5.
Raise an event if a SQL Server service restart succeeds?	Select **Yes** to raise an event if a SQL Server service restart succeeds. The default is Yes.

Parameter	How to Set It
Event severity if a SQL Server service restarts successfully	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a SQL Server service restarts successfully. The default is 30.
Raise an event if the Management Server service is not connected to the QDB?	Select **Yes** to raise an event if the Management Server service is not connected to the QDB. The default is Yes.
Event severity when the Management Server service is not connected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Management Server service is not connected. The default is 5.
Raise an event if the QDB SQL Server agent jobs are missing?	Select **Yes** to raise an event if the QDB SQL Server agent jobs are missing. The default is Yes.
Event severity for missing QDB SQL Server agent jobs	Set the event severity level, from 1 to 40, to indicate the importance of an event in which QDB SQL Server agent jobs are missing. The default is 15.
Raise an event if QDB SQL Server agent jobs are disabled?	Select **Yes** to raise an event if QDB SQL Server agent jobs are disabled. The default is Yes.
Event severity for disabled QDB SQL Server agent jobs	Set the event severity level, from 1 to 40, to indicate the importance of an event in which QDB SQL Server agent jobs are disabled. The default is 15.
Enable QDB SQL Server agent jobs if they are disabled?	Select **Yes** to enable QDB SQL Server agent jobs if they are disabled The default is Yes.
Event severity when the attempt to enable QDB SQL Server agent job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an attempt to enable QDB SQL Server agent job fails. The default is 15.
Raise an event if attempt to enable QDB SQL Server agent job succeeds?	Select **Yes** to raise an event if the attempt to enable the QDB SQL Server agent job succeeds. The default is unchecked.
Event severity when attempt to enable QDB SQL Server agent job succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an attempt to enable the QDB SQL Server agent job succeeds. The default is 20.
Raise an event if a QDB SQL Server agent job fails?	Select **Yes** to raise an event if a QDB SQL Server agent job fails**.** The default is Yes.
Event severity when a QDB SQL Server job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a QDB SQL Server job fails. The default is 20.
Raise an event if QDB disks are fragmented?	Select **Yes** to raise an event if AppManager detects QDB disk fragmentation. The default is unselected. **Tip** To avoid errors when running this script on a Windows Server 2008 server, disable User Account Control (UAC).
Event severity for QDB disk fragmentation	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a disk is fragmented. The default is 15.
Raise an event if the query process time exceeds threshold?	Select **Yes** to raise an event if the query process time exceeds threshold. The default is Yes.
Threshold -- Maximum process run time	Specify the longest process run time allowed before an event is raised. The default is 40 seconds.
Event severity when query process time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the query process time exceeds the threshold you set. The default is 5.

Parameter	How to Set It
Event severity when attempt to retrieve query process time fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the attempt to retrieve query process time fails. The default is 10.
Raise an event if unable to retrieve QDB component information?	Select **Yes** to raise an event if AppManager is unable to retrieve QDB component information. The default is Yes.
Event severity when unable to connect to retrieve QDB component information	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager is unable to connect to retrieve QDB component information. The default is 10.
Data Collection	
Collect data for database space utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of the database data file currently being used. The default is unselected.
Collect data for log space utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of the database log file currently being used. The default is unselected.
Collect data for Management Server connection status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns 100 if the Management Server is connected to the repository and 0 if the Management Server is not connected. The default is unselected.
Collect data for SQL Server service status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns 100 if the SQL Server service is up and 0 if the service is down. The default is unselected.
Monitoring	
SQL username	Specify the username required to access SQL Server on the Control Center server.
Management Server Performance Monitoring	
Raise an event if the Management Server map file is not enabled?	Select **Yes** to raise an event if the Management Server map file is not enabled. The default is Yes.
Threshold -- Current map file size	Specify the current map file size. If the map file size is too small, the Management Server performance will not be optimal in larger environments. The default is 5 MB.
Event severity if map file is not enabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the map file is not enabled. The default is 15.
Raise an event if data map file usage exceeds threshold?	Select **Yes** to raise an event if the data map file usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum data map file usage	Specify the highest level of data map file usage that can occur before an event is raised. The default is 80%.
Event severity when data map file usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data map file usage exceeds the threshold you set. The default is 15.
Raise an event if event map file usage exceeds threshold?	Select **Yes** to raise an event if the event map file usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum event map file utilization	Specify the highest level of event map file utilization that can occur before an event is raised. The default is 80%.
Event severity when event map file utilization exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the event map file utilization exceeds the threshold you set. The default is 15.

Parameter	How to Set It
Raise an event if job map file usage exceeds threshold?	Select **Yes** to raise an event if the job map file usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum job map file utilization	Specify the highest level of job map file utilization before an event is raised. The default is 80%.
Event severity when job map file usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job map file usage exceeds the threshold you set. The default is 15.
Collect data for Management Server data map file utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of the Management Server data map file currently being utilized. The default is unselected.
Collect data for Management Server event map file utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of the Management Server event map file currently being utilized. The default is unselected.
Collect data for Management Server job map file utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of the Management Server job map file currently being utilized. The default is unselected.
Monitoring SQL Server File Size and Growth Settings	
Raise an event if insufficient space available for further file growth?	Select **Yes** to raise an event if there is not enough space for additional file growth on the SQL Server. The default is Yes.
Event severity for insufficient space	Set the event severity level, from 1 to 40, to indicate the importance of an event in which there is not enough space for additional file growth on the SQL Server. The default is 10.
Raise an event if SQL Server file growth rate is lower than the threshold?	Select **Yes** to raise an event if the SQL Server file growth rate is lower than the threshold you set. The default is Yes.
Threshold -- Minimum growth rate in MB	Specify the lowest possible growth rate for the SQL Server in MB. The default is 256 MB.
Threshold -- Minimum growth rate as a percentage	Specify the lowest possible growth rate for the SQL Server as a percentage. The default is 9%.
Event severity when file growth rate is lower than the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the file growth rate is lower than the threshold you set. The default is 10.
Raise an event if SQL Server file size exceeds disk space	Select **Yes** to raise an event if the SQL Server file size exceeds the available disk space. The default is Yes.
Event severity when SQL Server file size exceeds disk space	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SQL Server file size exceeds the available disk space. The default is 15.
Raise an event if Autogrowth is not enabled and file utilization exceeds the threshold?	Select **Yes** to raise an event if Autogrowth is not enabled, and file utilization exceeds the threshold you set. The default is Yes.
Threshold -- Maximum file utilization with Autogrowth disabled	Specify the highest percentage of file utilization with Autogrowth disabled before an event is raised. The default is 90%.
Event severity if Autogrowth disabled and usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which usage exceeds the threshold and Autogrowth is disabled. The default is 10.
Event severity for a Knowledge Script error	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an unexpected Knowledge Script error occurs. The default is 10.

Parameter	How to Set It
Monitoring the Management Server Service	
Raise an event if the Management Server service is down?	Select **Yes** to raise an event if the Management Server service is down. The default is Yes.
Event severity if the Management Server service is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Management Server service is down The default is 15.
Restart the Management Server service if the service is down?	Select **Yes** if you want to restart the Management Server service if the service is down. The default is Yes.
Raise an event if the Management Server service restarts successfully?	Select **Yes** to raise an event if the Management Server service restarts successfully. The default is Yes.
Event severity if the Management Server service restarts successfully	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Management Server service restarts successfully. The default is 15.
Raise an event if the Management Server service fails to restart?	Select **Yes** to raise an event if the Management Server service fails to restart. The default is Yes.
Event severity if the Management Server service fails to restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Management Server service fails to restart. The default is 15.
Raise an event if agents are not FIPS-compliant?	Select **Yes** to raise an event if the agents are not FIPS-compliant. The default is Yes.
Event severity when agents are not FIPS-compliant	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the agents are not FIPS-compliant. The default is 10.

Recommended Knowledge Script Groups

You can find the AMHealth Knowledge Script Groups (KSGs) on the RECOMMENDED tab of the Knowledge Script pane in the Operator Console.

All the scripts in the KSGs have their parameters set to recommended values. To run all of the recommended scripts in a KSG at one time, click the RECOMMENDED tab, and then run the KSG on an AppManager resource.

The AMHealth KSGs enable a "best practices" usage for monitoring your AppManager environment. You can use these KSGs with AppManager monitoring policies. A monitoring policy lets you efficiently and consistently monitor all the resources in your environment using a set of pre-configured Knowledge Scripts. For more information, see "About Policy-Based Monitoring" in the AppManager Help.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the AMHealth tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the AMHealth tab are not affected.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the AMHealth KSG and want to restore it to its original form, you can reinstall the AppManager Self Monitoring module on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\AMHealth` directory.

HealthCheckAMAgentComponents Recommended KSG

The following Knowledge Scripts are members of the AgentComponents recommended KSG:

- HeartbeatUNIX
- HeartbeatWin

CoreComponents Recommended KSG

The following Knowledge Scripts are members of the CoreComponents recommended KSG:

- CCComponentsHealth
- QDBComponentsHealth

Chapter 8
Apache UNIX Knowledge Scripts

The AppManager for Apache UNIX category provides the following Knowledge Scripts for monitoring Apache UNIX servers.

From the Knowledge Script view of the Control Center Console, you can access more information about any NetIQ-supported Knowledge Script by selecting it and pressing F1. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press F1.

Knowledge Script	What It Does
AccessActivity	Monitors requests and the status codes of request errors.
AccessLogEntries	Monitors the number of new entries and content of new entries made to the access logs since last script execution.
Availability	Verifies that the root Apache process is running on an Apache Web Server or IBM HTTP Server.
ConfigFileUpdateCheck	Reports any configuration changes to Apache Web Servers and IBM HTTP Servers.
ConfigTest	Verifies the configuration of an Apache Web Server or IBM HTTP Server.
CoreDumpCheck	Checks for newly created core dump files on an Apache Web Server or IBM HTTP Server and reports the time the last file was created.
CPU	Monitors the percentage of CPU used by Apache processes.
ErrorLogEntries	Monitors the number of new entries and content of new entries made to the error logs since last script execution.
HealthCheck	Verifies Apache processes are running and servers are able to service requests.
InfoModule	Enables the mod_info module on an Apache Web Server or IBM HTTP Server. Most binary distributions disable this module by default.
KillLongRunningRequests	Kills requests that have been running longer than a specified time threshold.
KillProcessesAboveCPU	Kills runaway processes that are using too much CPU.
ModuleEnabled	Reports which Apache modules are enabled, which means they are loaded and active.
ProcessActivity	Monitors the status of HTTPD processes running on Apache Web Servers and IBM HTTP Servers.
Report_ActivitySummary	Generates a report summarizing the requests, requests by virtual hosts, and server utilization on monitored Apache Web Servers and IBM HTTP Servers.

Knowledge Script	What It Does
Report_HealthSummary	Generates a report summarizing the health of monitored Apache Web Servers and IBM HTTP Servers. This report includes information on availability, core files, error log entries, CPU, and virtual memory utilization.
Report_PerformanceSummary	Generates a report summarizing the throughput performance of monitored Apache Web Servers and IBM HTTP Servers.
Requests	Returns statistics on requests and request processing time data
ServerUtilization	Monitors the percentage of busy and idle processes on Apache Web Servers and IBM HTTP Servers.
StartServer	Starts or restarts specified Apache Web Servers or IBM HTTP Servers.
StatusModule	Enables the mod_status module on an Apache Web Server or IBM HTTP Server. Most binary distributions of Apache disable this module by default.
StopServer	Stops specified Apache Web Servers and IBM HTTP Servers.
Throughput	Returns statistics on throughput data.
TopNPageActivity	Lists the most popular Web pages on an Apache Web Server or IBM HTTP Server.
Uptime	Reports the time an Apache Web Server or IBM HTTP Server has been running. Uptime is reset if the Apache root process is killed for any reason.
VirtualMemory	Reports the total memory used by Apache processes, as well as returning this value as a percentage of total available memory.
Discovery_ApacheUNIX	Discovers Apache resource and configuration information on UNIX servers.

AccessActivity

Use this Knowledge Script to monitor access activity on Apache Web Servers and IBM HTTP Servers. This script returns information, such as status codes, about successful and failed requests.

You can use this script to determine which errors clients experience most frequently while accessing a server. This information is critical for maintaining and troubleshooting Web sites. For example, if the script returns multiple instances of status code 404 (file not found), you may have broken links or missing pages on your site.

To use this Knowledge Script, you must have the Apache CustomLog directive configured as `common` or `combined`. For information about how to configure the CustomLog directive, see your Apache documentation.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Daily at 2 AM**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if any threshold exceeded? (y/n)	Set to y to raise events. The default is y.
Event severity when script fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.
Event severity when any threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue event indicator.
Filter: regular expression	Specify a filter using a regular expression. This version supports filtering by virtual host only. The default is none.
Collect data for total requests? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the total number of requests to the Apache Web Server or IBM HTTP Server. The default is n.
Threshold -- Maximum total requests	Specify a threshold value using an integer greater than or equal to -1. If Total Requests exceed the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0.
Collect data for successes?	Set to y to collect data for charts and reports. If set to y, this script returns the number of successful requests to the Apache Web Server or IBM HTTP Server. The default is n.

Description	How to Set It
Threshold -- Maximum successes	Specify a threshold value using an integer greater than or equal to -1. If Successes exceed the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0.
Collect data for failures? (y/n)	Set to y to collect data for charts and reports. If set to y this script returns the number of failed requests to the Apache Web Server or IBM HTTP Server. The default is n.
Threshold--Maximum failures	Specify a threshold value using an integer greater than or equal to -1. If Failures exceed the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0.
Collect data for 3XX status codes? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the number of 3XX status codes. The default is n.
Threshold -- Maximum 3xx status codes	Specify a threshold value using an integer greater than or equal to -1. If the total number of 3XX status codes exceeds the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0.
Collect data for 4XX status codes? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the number of 4XX status codes. The default is n.
Threshold -- Maximum 4xx status codes	Specify a threshold value using an integer greater than or equal to -1. If the total number of 4XX status codes exceeds the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0.
Collect data for 5XX status codes? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the number of 5XX status codes. The default is n.
Threshold -- Maximum 5xx status codes	Specify a threshold value using an integer greater than or equal to -1. If the total number of 5XX status codes exceeds the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0.

AccessLogEntries

Use this Knowledge Script to monitor the number of new entries and the content of new entries made to the access logs since the last execution of this script. As long as the script is running as a regularly scheduled job, each time the script runs, AppManager only reports new entries that have appeared since the last time the script ran.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every 12 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if new access log entries detected? (y/n)	Set to y to raise events. The default is y.
Event severity when new access log entries detected	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue event indicator.
Filter: regular expression	Specify a regular expression value that the new entries, if present, must match before being reported as new entries.
Collect data for access log entries? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the number of new entries in the access logs since the last time the script ran. The default is n.
Raise event every time script executes and no new log entries are found? (y/n)?	Set to y to raise an event each time the script executes and no new error log entries are detected. The default is n.

Example of How this Script Is Used

If you want to only report new lines in the access log for 400 errors, you could specify "4[\d][\d]" for the Filter.

Availability

Use this Knowledge Script to monitor the availability (up/down status) of Apache Web Servers and IBM HTTP Servers by reporting the percentage of available servers. This script verifies that the root Apache process is running.

If the Apache Web Server or IBM HTTP Server is configured to run multiple root processes, the script reports the server as available (up) if any one of the processes is running, or unavailable (down) if none of the processes is running.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if process found not running? (y/n)	Set to y to raise events. The default is y.
Collect data for process status? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns 100% if the server is available (up), or 0% if the server is unavailable (down). The default is n.
Event severity when process not running	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.

ConfigFileUpdateCheck

Use this Knowledge Script to monitor changes to the Apache Web Server or IBM HTTP Server configuration files.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every 12 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if configuration changes detected? (y/n)	Set to y to raise events. The default is y.
Event severity when configuration changes detected	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue event indicator.
Raise event every time script executes? (y/n)	Set to y to raise an event at each iteration of the script. The default is n.

ConfigTest

Use this Knowledge Script to verify the syntax of the configuration file on an Apache Web Server or IBM HTTP Server. Invalid configuration can prevent the server from starting.

This script can be used to pinpoint configuration errors if, for example, the ExtendedStatus directive is on, but the status module is not enabled.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if configuration errors detected? (y/n)	Set to y to raise events. The default is y.
Event severity when script fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.
Event severity when script succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 35, which is the magenta event indicator.

CoreDumpCheck

Use this Knowledge Script to check if an Apache Web Server or IBM HTTP Server has created a core dump file since the last time this script was run. This script is useful to determine when an Apache Web Server or IBM HTTP Server failed.

This script looks for the core dump file in the directory where you installed Apache unless you specify a location of the core dump file using the CoreDumpDirectory Directive in the `httpd.conf` file.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if new core dump file detected? (y/n)	Set to y to raise events. The default is y.
Collect data for presence of core dump file? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns 100 if there is a core dump file, or 0 if there is no core dump file. The default is n.
Event severity when new core dump file detected	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue event indicator.
Event severity when script succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 35, which is the magenta event indicator.
Path to gdb	For computers running version 7.0 of the AppManager UNIX agent, specify the directory where the GNU debugger is located. This Knowledge Script does not require the debugger. The default is `/usr/bin/gdb`. This parameter is not supported on computers using the NetIQ UNIX Agent 7.1 and later.
Regular expression for name of the core dumped files	Specify the expression that defines the naming convention for the core dump files. Only set this parameter if you use a customized naming convention for core dump files. The default is `^core(\.\d+)?$`.

CPU

Use this Knowledge Script to monitor CPU activity by Apache processes.

This script is helpful in determining whether an Apache Web Server or IBM HTTP Server needs a more powerful processor.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if CPU utilization exceeds any threshold? (y/n)	Set to y to raise events. The default is y.
Event severity when CPU utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue event indicator.
Collect data for percentage of CPU load? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the percent of CPU load attributed to Apache processes. The default is n.
Threshold -- Maximum percentage of CPU load	Specify a threshold value using an integer greater than or equal to -1 and less than or equal to 100. If Apache processes exceed this threshold, an event is raised. Use -1 to ignore this threshold. The default is 0.
Collect data for total CPU time? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the total CPU time in seconds consumed by Apache processes. The default is n.
Threshold -- Maximum total CPU time	Specify a threshold value using an integer greater than or equal to -1. If Apache processes exceed this threshold, an event is raised. Use -1 to ignore this threshold. The default is 0.

ErrorLogEntries

Use this Knowledge Script to monitor the number of new entries and the content of new entries made to the error logs since the last execution of this script. As long as the script is running as a regularly scheduled job, each time the script runs, AppManager only reports new entries that have appeared since the last time the script ran.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every 12 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if new error log entries found? (y/n)	Set to y to raise events. The default is y.
Event severity when new error log entries detected	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the red event indicator.
Filter: regular expression	Specify a regular expression value that the new entries, if present, must match before being reported as new entries.
Collect data for error log entries? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the number of new error log entries. The default is n.
Raise event every time script executes and no new log entries are found? (y/n)?	Set to y to raise an event each time the script executes and no new error log entries are detected. The default is n.

Example of How this Script is Used

If you want to only report new lines in the error log that are critical, you can specify "crit" for the Filter.

HealthCheck

Use this Knowledge Script to make sure Apache processes are running and Apache Web Servers and IBM HTTP Servers are able to service requests. This script performs the following checks:

- Verifies all Apache processes (HTTPD processes) are running.
- Verifies the default page for each virtual host is available (status code 200).
- Verifies a list of specified URLs is available (status code 200). This script only checks the target page. This script does not verify pages that are linked from the target page, internal links to other locations in the target page, or pages that appear if the page automatically redirects to another URL when opened.

You can also use the HealthCheck script to:

- Restart servers if the script determines Apache processes are not running.
- Set response time thresholds for virtual hosts and URLs.
- Raise events with user-defined severity levels if Apache services are not running, or a virtual host or URL is not responding.

This Knowledge Script fails if you run the UNIX agent computer as a non-root user.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Daily at 2 AM**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise events? (y/n)	Set to y to raise events. The default is y.
Collect data for Web server process status? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns 100 if the HTTPD processes are running, or 0 if those process are not running. The default is n.
Event severity when script fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.
Event severity when threshold exceeded	You can set thresholds for virtual host and URL response times. Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue event indicator.
Restart server if process not running? (y/n)	Set to y to restart the server if Apache processes are not running. The default is y.
Event severity when Apache is not running	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.

Description	How to Set It
Check default page from each virtual host? (y/n)	Set to y to verify availability (status code 200) of the default pages from each virtual host. The default is y.
Threshold -- Maximum response time of virtual host	Specify a threshold value using an integer greater than or equal to -1. If virtual host response time (in ms) exceeds the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0 seconds.
Event severity when virtual host not responding	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 15 (yellow event indicator).

List of URLs to check (semicolon-separated, no spaces)	Specify a list of URLs to check for availability (status code 200). You must include full URLs, delimited by semicolons. Redirections, internal, and external links are not verified.
	When specifying a list of URLs to check, the following characters must be preceded by a backslash (\):
	• & (Ampersand)
	• ? (Question)
	• = (Equal)
	For example, an URL that contains:
	`login.asp?name=steve&password=pass`
	Must be specified as:
	`login.asp\?name\=steve\&password\=pass`
	The default is none.

Threshold -- Maximum response time for URL	Specify a threshold value using an integer greater than or equal to -1. If URL response time in milliseconds exceeds the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0 seconds.
Event severity when URL not responding	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 15, which is the yellow indicator.

InfoModule

Use this Knowledge Script to enable or disable Apache `mod_info` module. You must enable this module to verify Apache Web Server or IBM HTTP Server configuration at run time.

Running this Knowledge Script restarts the Apache Web Server or IBM HTTP Server.

This Knowledge Script fails if you run the UNIX agent computer as a non-root user.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if script succeeds or fails? (y/n)	Set to y to raise events. The default is y.
Enable `mod_info`? (y/n)	Set to y to enable Apache `mod_info` module. The default is y.
Event severity when script succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 35, which is the magenta event indicator.
Event severity when script fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.
Path to module (may be relative to `serverRoot;semicolon-separated,no spaces`)	Specify the directory path of the `mod_info` module. The default is `modules;libexec`.

KillLongRunningRequests

Use this Knowledge Script to terminate requests that run longer than their allotted threshold. If your web server contains a multi-processing module, such as the worker MPM, each process may contain more than one thread processing a request. If this Knowledge Script terminates a requests on one thread, then the requests on the other threads are also terminated.

On computers running version 7.0 of the AppManager UNIX agent, you must run the Install Knowledge Script before you run this Knowledge Script.

This Knowledge Script fails if you run the UNIX agent computer as a non-root user.

This Knowledge Script is only supported for Apache Web Server 2.0 and 2.2. Apache Web Server version 1.3 reports request time differently than later versions. If you run this Knowledge Script on a computer running Apache Web Server 1.3, AppManager will terminate requests significantly before your defined threshold.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if time request has been running exceeds threshold? (y/n)	Set to y to raise events. The default is y.
Collect data for number of killed requests? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the number of killed requests. If your server uses the multi-processing module, all requests that belong to the same process are terminated together, so this data does not necessarily represent the number of long running requests. The default is n.
Threshold -- Maximum time request can run	Specify a threshold value, in seconds, using an integer greater than or equal to -1. If a single request exceeds the threshold value, the request is killed and an event is raised. Use -1 to ignore this threshold. The default is 900 seconds.
Event severity when processes are killed	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 20, which is the yellow event indicator.

KillProcessesAboveCPU

Use this Knowledge Script to kill processes that exceed either the CPU time or CPU percentage threshold. For each process that exceeds a threshold, the event detail message includes the process name, the percentage of CPU used, the CPU time used, and whether the attempt to kill the process was successful or not. If your web server contains the multi-processing module, this Knowledge Script terminates all requests that belong to the same process as the request that runs longer than its allotted threshold.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if any threshold exceeded or process killed? (y/n)	Set to y to raise events. The default is y.
Collect data for number of processes killed? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the number of process that were killed. The default is n.
Number of samples to take	Specify the number of times to sample the CPU process list. The default is 10.
Delay between samples	Specify an interval, in seconds, between each sampling of the CPU process list. The default is 1 second.
Threshold -- Number of samples exceeding threshold before process killed	This threshold determines how many samples, out of the total number of samples specified above, must exceed the threshold of either CPU percentage or CPU time for a process to be killed. The default is 10 samples.
Threshold -- Maximum CPU utilization (percentage)	Specify a threshold value, in percent, using an integer greater than or equal to -1 and less than or equal to 100. If an Apache process exceeds this threshold, an event is raised. Use -1 to ignore this threshold. The default is 95 percent.
Threshold -- Maximum CPU utilization (time)	Specify a threshold value, in seconds, using an integer greater than or equal to -1. If an Apache process exceeds this threshold, an event is raised. Use -1 to ignore this threshold. The default is 100 seconds.
Event severity when processes are killed	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 20, which is the yellow event indicator.

ModuleEnabled

Use this Knowledge Script to verify whether a specified Apache Web Server or IBM HTTP Server module is enabled, which means the module is loaded and active.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if module enabled or disabled? (y/n)	Set to y to raise events. The default is y.
Event severity when module is enabled	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 35, which is the magenta event indicator.
Event severity when module is disabled	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 20.
Names of modules to test (semicolon-separated, no spaces)	Specify a list of module names, separated by semicolons, to test for enabled status. The default is `mod_status;mod_info;mod_nqApache223`.
Source names for modules to test (semicolon-separated, no spaces)	For computers running version 7.0 of the AppManager UNIX agent, specify a list of source names, separated by semicolons, to test for enabled status. This parameter is not supported on computers using the NetIQ UNIX Agent 7.1 and later. The default is `mod_status;mod_info;mod_nqApache223`.

ProcessActivity

Use this Knowledge Script to monitor the percentage of Apache processes that are serving requests for each virtual host on the server, and for each unique client.

You can use this script to help determine if you are under a denial-of-service attack, for example, if a single client is using an excessive percentage of processes.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if process usage exceeds any threshold? (y/n)	Set to y to raise events. The default is y.
Event severity when script fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.
Event severity when process usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue event indicator.
Time frame to monitor (times less than supplied value are monitored)	Specify an integer less than or equal to 86400. The units are measured in seconds. The default is 60. HTTPD processes whose most recent request is greater than the specified value are ignored. This allows the script to discount HTTPD processes that have not run within the time window of interest. If this parameter is set to 0, the script will consider all requests during the previous 24 hours.
Collect data per virtual host? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the percentage of HTTPD process used by each virtual host. The default is n.
Threshold -- Maximum percentage of processes per virtual host	Specify a threshold value using an integer greater than or equal to -1. If a single virtual host exceeds this threshold (percentage of HTTPD processes), an event is raised. Use -1 to ignore this threshold. The default is 0 percentage of HTTPD processes.
Collect data per common client? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the percentage of HTTPD processes used by each common client. The default is n.
Threshold -- Maximum percentage of processes per common client	Specify a threshold value using an integer greater than or equal to -1. If a common client exceeds this threshold (percentage of HTTPD processes), an event is raised. Use -1 to ignore this threshold. The default is 0 percentage of HTTPD processes.

Report_ActivitySummary

Use this Report Script to generate a report summarizing the activity of monitored Apache Web Servers and IBM HTTP Servers. The report provides data on the number of total requests and the percentage of processes that are busy and that are on each virtual host.

This Knowledge Script uses data other scripts collect. Before you run this Knowledge Script, you must first run the Throughput, ProcessActivity, and ServerUtilization Knoweldge Scripts.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report. The default is Sliding Time: 1 Day; End Now = No
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report. The default is Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
Aggregation by	Select the time period (Hour, Minute, or Day) by which the data in your report is aggregated. The default is Hour.
Aggregation interval	Select the interval between aggregations of the data in your report. This parameter uses the time period specified in the **Aggregation by** parameter to calculate the interval. The default is 1.
Report Component Selection	Use the following parameters to define which data and statistics are displayed in the report.
Include parameter card?	Set to yes to include a card in the report that lists parameter settings for the report script. The default is yes.
Include Total Requests detail table?	Set to yes to include data from the Total Requests detail table in the report. The default is yes.
Include Total Requests chart?	Set to yes to include data from the Total Requests chart in the report. The default is yes.

Description	How to Set It
Threshold on Total Requests chart	Specify an integer to set a threshold for the Total Requests chart. Use -1 to ignore this threshold. The default is 0.
Include Processes per Virtual Host detail table?	Set to yes to include data from the Processes per Virtual Host detail table in the report. The default is yes.
Include Processes per Virtual Host chart?	Set to yes to include data from the Processes per Virtual Host chart in the report. The default is yes.
Threshold on Processes per Virtual Host chart	Specify an integer to set a threshold for the Processes per Virtual Host chart. Use -1 to ignore this threshold. The default is 0.
Include Busy Processes detail table?	Set to yes to include data from the Busy Processes detail table in the report. The default is yes.
Include Busy Processes chart?	Set to yes to include data from the Busy Processes chart in the report. The default is yes.
Threshold on Busy Processes chart	Specify an integer to set a threshold for the Busy Processes chart. Use -1 to ignore this threshold. The default is 0.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Customize chart appearance	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report. The default is Ribbon.
Select report location	Click the **Browse [...]** button to open the Publishing Options dialog box. Define the report filename and specify a default folder for this report. The default is ApacheUNIX_ActivitySummary.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Index-Report Title	Click in the Value column, and click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired. The default title is ApacheUNIX Activity Summary.
Add time stamp to title	Set to yes to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Raise event for report success?	Set to yes to raise an event when the report is successfully generated. The default is yes.

Description	How to Set It
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 35, which is the magenta level indicator.
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue level indicator.
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5, which is the red level indicator.

Report_HealthSummary

Use this Report Script to generate a report summarizing the health of monitored Apache Web Servers and IBM HTTP Servers. The report provides data on the following:

- Availability
- Core Files
- Error Log Entries
- CPU
- Virtual Memory Utilization

This Knowledge Script uses data other scripts collect. Before you run this Knowledge Script, you must first run the Throughput, ProcessActivity, and ServerUtilization Knoweldge Scripts.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report. The default is Sliding Time: 1 Day; End Now = No.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report. The default is Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
Aggregation by	Select the time period (Hour, Minute, or Day) by which the data in your report is aggregated. The default is Hour.
Aggregation interval	Select the interval between aggregations of the data in your report. This parameter uses the time period specified in the **Aggregation by** parameter to calculate the interval. The default is 1.
Report Component Selection	Use the following parameters to define which data and statistics are displayed in the report.
Include parameter card?	Set to yes to include a card in the report that lists parameter settings for the report script. The default is yes.

Description	How to Set It
Include Availability detail table?	Set to yes to include data from the Availability detail table in the report. The default is yes.
Include Availability chart?	Set to yes to include data from the Availability chart in the report. The default is yes.
Threshold on Availability chart	Specify an integer to set a threshold for the Availability chart. Use -1 to ignore this threshold. The default is 0.
Include Core Files detail table?	Set to yes to include data from the Core Files detail table in the report. The default is yes.
Include Core Files chart?	Set to yes to include data from the Core Files chart in the report. The default is yes.
Threshold on Core Files chart	Specify an integer to set a threshold for the Core Files chart. Use -1 to ignore this threshold. The default is 0.
Include Error Log Entries detail table?	Set to yes to include data from the Error Log Entries detail table in the report. The default is yes.
Include Error Log Entries chart?	Set to yes to include data from the Error Log Entries chart in the report. The default is yes.
Threshold on Error Log Entries chart	Specify an integer to set a threshold for the Error Log Entries chart. Use -1 to ignore this threshold. The default is 0.
Include CPU Utilization detail table?	Set to yes to include data from the CPU Utilization detail table in the report. The default is yes.
Include CPU Utilization chart?	Set to yes to include data from the CPU Utilization chart in the report. The default is yes.
Threshold on CPU Utilization chart	Specify an integer to set a threshold for the CPU Utilization chart. Use -1 to ignore this threshold. The default is 0.
Include Virtual Memory detail table?	Set to yes to include data from the Virtual Memory detail table in the report. The default is yes.
Include Virtual Memory chart?	Set to yes to include data from the Virtual Memory chart in the report. The default is yes.
Threshold on Virtual Memory chart	Specify an integer to set a threshold for the Virtual Memory chart. Use -1 to ignore this threshold. The default is 0.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Customize chart appearance	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report. The default is Ribbon.
Select report location	Click the **Browse [...]** button to open the Publishing Options dialog box. Define the report filename and specify a default folder for this report. The default is ApacheUNIX_HealthSummary

Description	How to Set It
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Index-Report Title	Click in the Value column, and click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired The default title is ApacheUnix Health Summary.
Add time stamp to title	Set to yes to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Raise event for report success?	Set to yes to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 35, which is the magenta level indicator.
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue level indicator.
Severity level for report failure.	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5, which is the red level indicator.

Report_PerformanceSummary

Use this Report Script to generate a report summarizing the throughput performance of monitored Apache Web Servers and IBM HTTP Servers.

This Knowledge Script uses data other scripts collect. Before you run this Knowledge Script, you must first run the Throughput, ProcessActivity, and ServerUtilization Knoweldge Scripts.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report. The default is Sliding Time: 1 Day; End Now = No.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report. The default is Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
Aggregation by	Select the time period (Hour, Minute, or Day) by which the data in your report is aggregated. The default is Hour.
Aggregation interval	Select the interval between aggregations of the data in your report. This parameter uses the time period specified in the **Aggregation by** parameter to calculate the interval. The default is 1.
Report Component Selection	Use the following parameters to define which data and statistics are displayed in the report.
Include parameter help card?	Set to yes to include a card in the report that lists parameter settings for the report script. The default is yes.
Include Throughput (req/s) detail table?	Set to yes to include data from the Throughput (req/s) detail table in the report. The default is yes.
Include Throughput (req/s) chart?	Set to yes to include data from the Throughput (req/s) chart in the report. The default is yes.

Description	How to Set It
Threshold on Throughput (req/s) chart	Specify an integer to set a threshold for the Throughput (req/s) chart. Use -1 to ignore this threshold. The default is 0.
Include Throughput (bytes/s) detail table?	Set to yes to include data from the Throughput (bytes/s) detail table in the report. The default is yes.
Include Throughput (bytes/s) chart?	Set to yes to include data from the Throughput (bytes/s) chart in the report. The default is yes.
Threshold on Throughput (bytes/s) chart	Specify an integer to set a threshold for the Throughput (bytes/s) chart. Use -1 to ignore this threshold. The default is 0.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Customize chart appearance	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report. The default is Ribbon.
Select report location	Click the **Browse [...]** button to open the Publishing Options dialog box. Define the report filename and specify a default folder for this report. The default is ApacheUNIX_PerformanceSummary.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Index-Report Title	Click in the Value column, and click the **Browse (...)** button to open the Report Properties dialog box. Set the properties parameters as desired. The default title is ApacheUNIX Performance Summary.
Add time stamp to title	Set to yes to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Raise event for report success?	Set to yes to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 35, which is the magenta level indicator.
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue level indicator.
Severity level for report failure.	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 5, which is the red level indicator.

Requests

Use this Knowledge Script to monitor:

- Maximum processing time
- Average processing time
- Average accesses per connection

You can use this script in capacity planning. For example, if processing time for requests is too long, you may want to upgrade the computer to support the level of Web traffic, or limit the number of other applications running on the computer.

You can also use this script to determine whether enough child processes are being spawned to handle the number of requests. If the data returned for average accesses per connection indicates that each child process is handling too many requests, you can alter your configuration of the server.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Daily at 2 AM**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if any threshold exceeded? (y/n)	Set to y to raise events. The default is y.
Event severity when script fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue event indicator.
Collect data for maximum processing time? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the maximum request processing time (in ms) for the last interval. The default is n.
Threshold -- Maximum processing time	Specify a threshold value using an integer greater than or equal to -1. If the maximum processing time in milliseconds exceeds this threshold, an event is raised. Use -1 to ignore this threshold. The default is 0 milliseconds.
Collect data for average processing time? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the average processing time in milliseconds per request during the last interval. The default is n.

Description	How to Set It
Threshold -- Maximum average processing time	Specify a threshold value using an integer greater than or equal to -1. If the average processing time in milliseconds exceeds this threshold, an event is raised. Use -1 to ignore this threshold. The default is 0 milliseconds.
Collect data for average accesses per connection? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the average number of accesses per connection, which is the average number of requests handled by each child process. The default is n.
Threshold -- Maximum average accesses per connection	Specify a threshold value using an integer greater than or equal to -1. If the average accesses per connection exceeds this threshold, an event is raised. Use -1 to ignore this threshold. The default is 0.

ServerUtilization

Use this Knowledge Script to monitor the utilization statistics for Apache Web Servers and IBM HTTP Servers. This Knowledge Script tracks the percentage of busy and idle processes on specified servers.

You can use this Knowledge Script to track how busy a server is at a given time. For example, if a server is overutilized, you may want to increase the number of HTTPD processes it is running.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if any threshold exceeded? (y/n)	Set to y to raise events. The default is y.
Event severity when script fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.
Event severity when any threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue event indicator.
Collect data for percentage of processes busy? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the percentage of busy processes. The default is n.
Threshold -- Maximum percentage of processes busy	Specify a threshold value using an integer greater than or equal to -1. If the percentage of busy processes exceeds this threshold, an event is raised. Use -1 to ignore this threshold. The default is 0 percent.
Collect data for number of busy processes? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the number of busy processes. The default is n.
Threshold -- Maximum number of busy processes	Specify a threshold value using an integer greater than or equal to -1. If the number of busy processes exceeds this threshold, an event is raised. Use -1 to ignore this threshold. The default is 0 busy processes.
Collect data for number of idle processes? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the number of idle processes. The default is n.
Threshold -- Maximum number of idle processes	Specify a threshold value using an integer greater than or equal to -1. If the number of idle processes exceeds this threshold, an event is raised. Use -1 to ignore this threshold. The default is 0 idle processes.

Description	How to Set It
Collect data for percentage of allowed requests per child? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the percentage of allowed requests. The default is n.
Threshold -- Maximum percentage allowed requests per child	Specify a threshold value using an integer greater than or equal to -1. If the percentage of allowed requests per child exceeds this threshold, an event is raised. Use -1 to ignore this threshold. The default is 0 percent.
Collect data for percentage of allowed servers? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the percentage of allowed servers. The default is n.
Threshold -- Maximum percentage of allowed servers	Specify a threshold value using an integer greater than or equal to -1. If the percentage of allowed servers realized exceeds this threshold, an event is raised. Use -1 to ignore this threshold. The default is 0 percent.

StartServer

Use this Knowledge Script to start or restart Apache Web Servers and IBM HTTP Servers.

You can use this Knowledge Script as a maintenance tool for remote restarting of Apache Web Servers and IBM HTTP Servers. For example, you can use the default schedule to stop and restart all Apache Web Servers each day at 3:00 A.M. to halt runaway processes.

This Knowledge Script fails if you run the UNIX agent computer as a non-root user.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Daily at 3 AM**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if script succeeds or fails? (y/n)	Set to y to raise events. The default is y.
Collect data for job successful or unsuccessful? (y/n)	Set to y to collect data for reports and graphs. If set to y, this script returns 100 if a restart is successful, or 0 if it is unsuccessful. The default is n.
Event severity when script fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.
Event severity when script succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 35, which is the magenta event indicator.
Method to use when starting Apache server	Specify a method for starting the specified server: • **Start**: starts the server. • **Restart**: stops running processes immediately and restarts the server. • **Graceful**: allows running processes to finish requests, then restarts the server. The default is Graceful.

StatusModule

Use this Knowledge Script to enable or disable the `mod_status` module on an Apache Web Server or IBM HTTP Server. You must enable this module for some monitoring Knowledge Scripts to return data. Running this Knowledge Script will restart the Apache Web Server or IBM HTTP Server.

This Knowledge Script fails if you run the UNIX agent computer as a non-root user.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if script succeeds or fails? (y/n)	Set to y to raise events. The default is y.
Enable `mod_status`? (y/n)	Set to y to enable Apache `mod_status` module. The default is y.
Event severity when enabling or disabling succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 35, which is the magenta event indicator.
Event severity when enabling or disabling fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.
Path to module (may be relative to `serverRoot;semicolon-separated,no spaces`)	Specify the directory path of the `mod_status` module. The default is `modules;libexec`.

StopServer

Use this Knowledge Script to stop an Apache Web Server or IBM HTTP Server that is currently running.

This Knowledge Script lets you specify whether to kill running processes and stop the server immediately, or allow processes to finish requests before stopping the server.

You can use this Knowledge Script in conjunction with another script as a troubleshooting tool. For example, if the ProcessActivity Knowledge Script determines that a server is experiencing a denial-of-service attack, the StopServer script can be invoked to stop the server immediately.

This Knowledge Script fails if you run the UNIX agent computer as a non-root user.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Daily at 3 AM**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if script succeeds or fails? (y/n)	Set to y to raise events. The default is y.
Collect data for job successful or unsuccessful? (y/n)	Set to y to collect data for charts and reports. If set to y, the script returns 100 if a server is stopped, or 0 if a server is not stopped. The default is n.
Method to use when stopping Apache server	Specify a method for starting the specified servers: • **Stop**: stops running processes, finalizes dependencies, then closes dependencies. • **Graceful-stop**: allows running processes to finish requests, then stops the server. This option is not supported on Apache Web Server 1.3 and 2.0. • **Enforced**: stops running processes and dependencies immediately, without properly finalizing dependencies. The default is Stop.
Event severity when script fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.
Event severity when script succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 35, which is the magenta event indicator.

Throughput

Use this Knowledge Script to monitor throughput statistics for Apache Web Servers and IBM HTTP Servers. This Knowledge Script collects data on total bytes, total accesses, requests per second, bytes per second, and bytes per request.

You can use this Knowledge Script to monitor how quickly and efficiently requested data is returned to clients by the Apache Web Server or IBM HTTP Server.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if any threshold exceeded? (y/n)	Set to y to raise events. The default is y.
Event severity when script fails	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10, which is the red event indicator.
Event severity when threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25, which is the blue event indicator.
Source of throughput data	For computers running version 7.0 of the AppManager UNIX agent, specify the information source the script uses to collect throughput data: • NetIQ Apache Agent • mod_status • Any If you select Any, the script attempts to use NetIQ Apache Agent. If the agent is unavailable, mod_status is used. If neither is available, AppManager reports an error. This parameter is not supported on computers using the NetIQ UNIX Agent 7.1 and later.
Collect data for total bytes? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the total number of bytes. The default is n.
Threshold -- Maximum total bytes	Specify a threshold value using an integer greater than or equal to -1.If total bytes exceed the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0 bytes.
Collect data for total accesses? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the total number of accesses. The default is n.

Description	How to Set It
Threshold -- Maximum total accesses	Specify a threshold value using an integer greater than or equal to -1. If total accesses exceed the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0 accesses.
Collect data for requests per second? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the number of requests per second. The default is n.
Threshold--Maximum requests per second	Specify a threshold value using an integer greater than or equal to -1. If requests per second exceed the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0 requests.
Collect data for bytes per second? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the number of bytes per second. The default is n.
Threshold--Maximum bytes per second	Specify a threshold value using an integer greater than or equal to -1. If bytes per second exceed the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0 bytes.
Collect data for bytes per request? (y/n)	Set to y to collect data for charts and reports. if set to y, this script returns the number of bytes per request. The default is n.
Threshold--Maximum bytes per request	Specify a threshold value using an integer greater than or equal to -1. If bytes per request exceed the threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0 bytes.

TopNPageActivity

Use this Knowledge Script to monitor the pages with the most activity on an Apache Web Server or IBM HTTP Server.

To use this Knowledge Script, you must have the Apache CustomLog directive configured as `common` or `combined`. For information about how to configure the CustomLog directive, see your Apache documentation.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise events? (y/n)	Set to y to raise events. The default is y.
Collect data for number of times each page accessed? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the number of times each monitored page was accessed during the interval. The default is n.
Number of pages with highest activity to monitor	Specify the number of most popular Web pages, which are the pages with the most activity, to list. The default is 5.
Filter: virtual hostname or filename of requests	Specify a filter using a regular expression for matching against the virtual host name and filename of requests. If you are using a virtual host, you must specify an access log for the virtual host using the Apache CustomLog directive.

Uptime

Use this Knowledge Script to monitor the time that an Apache Web Server or IBM HTTP Server has been running.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if server uptime counter resets? (y/n)	Set to y to raise events. The default is y.
Collect data for server uptime? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the amount of time in seconds the server has been running since its last start. The default is n.
Event severity when uptime counter resets	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 30.
Source of uptime data	For computers running version 7.0 of the AppManager UNIX agent, specify the information source the script uses to collect uptime data: • NetIQ Apache Agent • mod_status • Any If you select Any, the script attempts to use NetIQ Apache Agent. If the agent is unavailable, mod_status is used. If neither is available, AppManager reports an error. This parameter is not supported on computers using the NetIQ UNIX Agent 7.1 and later.

VirtualMemory

Use this Knowledge Script to monitor virtual memory use, in percent and kilobytes, on an Apache Web Server or IBM HTTP Server.

Resource Objects

Apache Web Server or IBM HTTP Server

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if any threshold exceeded? (y/n)	Set to y to raise events. The default is y.
Event severity when virtual memory utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Collect data for percentage of virtual memory used? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the percentage of virtual memory used by the Apache Web Server or IBM HTTP Server. The default is n.
Threshold -- Maximum virtual memory utilization (%)	Specify a threshold value using an integer greater than or equal to -1and lesser than or equal to 100. If Apache processes exceed the percentage threshold, an event is raised. Use -1 to ignore this threshold. The default is 0 percent.
Collect data for total virtual memory used? (y/n)	Set to y to collect data for charts and reports. If set to y, this script returns the amount of virtual memory in kilobytes used by the Apache Web Server or IBM HTTP Server. The default is n.
Threshold -- Maximum virtual memory utilization (KB)	Specify a threshold value using an integer greater than or equal to -1. If Apache processes exceed the KB threshold value, an event is raised. Use -1 to ignore this threshold. The default is 0 KB.

Discovery_ApacheUNIX

Use this Knowledge Script to discover Apache Web Servers and IBM HTTP Servers installed on UNIX servers. This Knowledge Script returns information about successful, failed, and partial discoveries and raises events with user-specified severity to notify you of errors.

You can use this Knowledge Script to determine if and where Apache Web Servers and IBM HTTP Servers are installed in a UNIX network. Run this Knowledge Script periodically to detect new instances of Apache Web Servers and IBM HTTP Servers and to determine if existing servers have been uninstalled or taken offline.

Resource Object

UNIX computer with Apache Web Server or IBM HTTP Server.

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise an event for successful discovery? (y/n)	Set to y to raise an event when the Knowledge Script discovers an Apache Web Server or IBM HTTP Server. The default is n.
Event severity when Discovery succeeds	Specify a severity level for the event raised by successful discovery of an Apache Web Server or IBM HTTP Server. The default is 25.
Event severity when Discovery fails	Specify a severity level for the event raised by failure to discover an Apache Web Server or IBM HTTP Server. The default is 5.
Event severity when Discovery is partially successful	Specify a severity level for the event raised when the Knowledge Script starts but does not run to completion. The default is 15.
Paths to search for the Apache binary program (semicolon-separated, no spaces)	Use this variable to expedite the discovery process. Specify a directory path or list of paths separated by a semicolon. The Knowledge Script will limit its search for the Apache binary program to the paths you specify. The default is `/usr/local/apache2/bin/httpd`.
Paths for the Apache configuration files (Semicolon-separated, no spaces)	Use this variable to expedite the discovery process. Specify a directory path or list of paths separated by a semicolon. The Knowledge Script will limit its search for the Apache configuration files to the paths you specify. The default is `/usr/local/apache2/conf/httpd.conf`.
Paths to search for the Apache management script (`semicolon-separated,no spaces`)	Use this variable to expediate the discovery process. Specify a directory path or list of paths separated by a semicolon. The Knowledge Script will limit its search for the Apache management script, `apachectl`. The default is `/usr/local/apache2/bin/apachectl`.

Chapter 9
Application Knowledge Scripts

The Application category provides the following Knowledge Scripts for monitoring user-defined applications, including internally developed applications.

From the Knowledge Script view of Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ApplicationDown	Monitors application processes.
CpuHigh	Monitors the CPU resources an application's processes are consuming.
MemoryHigh	Monitors the memory an application's processes are consuming.

ApplicationDown

Use this Knowledge Script to check whether application processes are running. This script checks the running status of the processes for each application and raises an event if any application process is not running.

If the application is not on the local computer, the AppManager agent service must run as a domain account with appropriate access rights to access the remote application. In addition, you may need to map a drive name to the remote computer before running this Knowledge Script.

Resource Object

Application executable (`.exe` or `.com`)

Default Schedule

The default schedule is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Event severity if applications are not running	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 18 (yellow event indicator).

CpuHigh

Use this Knowledge Script to monitor the CPU resources that application processes are consuming. This script raises an event if an application's CPU utilization exceeds the thresholds you set. In addition, this script monitors CPU usage for each process individually and the total CPU usage for all processes. If a process is not found, the script assumes that the process is not currently running, and reports zero as the CPU result.

Resource Objects

Application executable, Application server

Default Schedule

The default schedule is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Event for each process?	Set to **y** to raise events. The default is y.
CPU usage threshold for each process	Enter the maximum amount of CPU usage that each process can consume before an event is raised. The default is 60%.
Collect data for each process?	Set to **y** to collect data for individual processes. If set to y, this script returns the amount of CPU usage each process consumes. The default is n.
Event for all processes?	Set to **y** to raise events. The default is y.
CPU usage threshold for all processes	Enter the maximum amount of CPU usage that all processes can consume before an event is raised. The default is 95%.
Collect data for all processes?	Set to **y** to collect data for all processes you are monitoring. If set to y, this script returns the amount of CPU usage all processes are consuming. The default is n.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 8 (red event indicator).

MemoryHigh

Use this Knowledge Script to monitor the memory an application's processes are consuming. This script checks the memory used by each process individually, and the total memory used by all processes. If a process is not found, it assumes that the process is not currently running, and reports zero as the memory result.

Resource Objects

Application executable, Application server

Default Schedule

The default schedule is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Event for each process?	Set to **y** to raise events. The default is y.
Memory usage threshold for each process	Enter the maximum amount of memory usage that each process can consume before an event is raised. The default is 20000 KB.
Collect data for each process?	Set to **y** to collect data for all processes you are monitoring. If set to y, this script returns the amount of memory usage each process is consuming. The default is n.
Event for all processes?	Set to **y** to raise events. The default is y.
Memory usage threshold for all processes	Enter the maximum amount of memory usage that all processes can consume before an event is raised. The default is 32000 KB.
Collect data for all processes?	Set to **y** to collect data for all processes you are monitoring. If set to y, this script returns the amount of memory usage all processes are consuming. The default is n.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 8 (red event indicator).

Chapter 10
ARCserve Knowledge Scripts

The CA ARCserve category provides the following Knowledge Scripts for monitoring CA ARCserve.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ActivityLogSize	Monitors the size of the ARCserve Activity log.
AlertMediaChange	Monitors the number of jobs that are currently waiting for a change of medium before a backup can proceed.
CanceledJobs	Monitors the number of canceled ARCserve jobs.
DeleteJobs	Deletes all jobs or specified types of jobs from the job queue.
EventLog	Scans the Windows Application event log for entries created by ARCserve and returns data about those entries.
FailedJobs	Monitors the number of failed ARCserve jobs.
HungJobs	Checks for backup jobs that started but did not finish.
IncompleteJobs	Monitors the number of incomplete ARCserve jobs.
LogFiles	Monitors the number of log files ARCserve has generated in its Log directory; also deletes old log files.
Report_ActivityLogSize	Generates a report about the size of the ARCserve Activity log.
Report_CPUandMemoryUsage	Generates a report about the CPU and memory utilization of ARCserver services.
Report_NumberofCanceledJobs	Generates a report about the number of canceled ARCserve jobs.
Report_NumberofFailedJobs	Generates a report about the number of failed ARCserve jobs.
Report_NumberofIncompleteJobs	Generates a report about the number of incomplete ARCserve jobs.
Report_NumberofSuccessfulJobs	Generates a report about the number of successful ARCserve jobs.
RescheduleJobs	Adjusts the scheduled run time of all jobs in the ARCserve job queue.
ResourceHigh	Monitors the CPU and memory utilization of ARCserve services.
ServiceDown	Monitors ARCserve services to see if they are running.

Knowledge Script	What It Does
SetLoggingType	Configures ARCserve to write event information to the Windows Application event log.
SuccessfulJobs	Monitors the number of successful ARCserve jobs.

ActivityLogSize

Use this Knowledge Script to monitor the size of the ARCserve Activity log file (`ARCserve.log`). When the size of the log exceeds the threshold you set, an event is raised.

Note
If both ARCserve and ARCserveIT are installed on the same computer, only the ARCserveIT Activity log is monitored.

Resource Objects

ARCserve server, ARCserveIT server

Default Schedule

The default schedule is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. When set to y, returns the size of the Activity Log in megabytes (MB). The default is n.
Maximum threshold for log file	Enter the maximum size that the Activity Log file can reach before an event is raised. The default is 1000 MB.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

AlertMediaChange

Use this Knowledge Script to search the ARCserve log for messages indicating that jobs that are currently waiting for a change of medium before a backup can proceed. If the number of jobs exceeds the threshold you set, an event is raised.

When a backup job pauses to wait for new backup media such as, a tape drive to become available, it writes a media alert message to the log file (`ARCserve.log`). The same job may write multiple media alert entries in the log while it is waiting, and then it may continue when the medium becomes available. You can set the threshold to a value that indicates a job has been waiting for a long time while issuing multiple alerts, or that many jobs are waiting. Or, if you want this Knowledge Script to raise an event anytime it detects even one media alert entry in the log, set the threshold to 0.

Note
If both ARCserve and ARCserveIT are installed on the same computer, only the ARCserveIT Activity log is monitored.

Resource Objects

ARCserve server, ARCserveIT server

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. When set to **y**, returns the number of media alerts found in the log during the current interval. The default is n.
Start with new entries?	This parameter controls what the Knowledge Script does on its first iteration: • If set to **y**, this script does not scan existing entries on its first iteration, and therefore it does not raise events or collect data on its first iteration. On subsequent iterations, this script only scans new entries written to the log file since the last monitoring interval. • If set to **n**, this script scans all existing entries on its first iteration and therefore can raise events and collect data on its first interval. On subsequent iterations, this script only scans new entries written to the log file since the last monitoring interval. The default is n.
Maximum threshold for media alerts	Enter the maximum number of media alert messages allowed during any single scan of the ARCserve log file before an event is raised. If you specify 0, the script raises an event when it finds any media alerts. The default is 0 alert messages.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

CanceledJobs

Use this Knowledge Script to check for canceled ARCserve jobs and to return data about those jobs.

This script periodically scans the latest ARCserve Activity log file (`ARCserve.log`) for entries that indicate a job was canceled. If, during any monitoring interval, the number of canceled jobs found in the `ARCserve.log` file exceeds the threshold you set, an event is raised.

When an event is raised, the contents of the event detail message depend on whether you are also collecting data. When the Knowledge Script is collecting data, the event detail message reports the number of canceled jobs. The data detail message contains the actual log entries. When the Knowledge Script is not collecting data, the event detail message returns all of the log entries related to canceled jobs.

Note
If both ARCserve and ARCserveIT are installed on the same computer, only the ARCserveIT jobs are monitored.

Resource Objects

ARCserve server, ARCserveIT server

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of canceled jobs. The default is n.
Start with new entries?	This parameter controls what the Knowledge Script does on its first iteration: • If set to **y**, this script does not scan existing entries on its first iteration, and therefore does not raise events or collect data on its first iteration. On subsequent iterations, this script only scans the new entries that are written to the log file since the last monitoring interval. • If set to n, this script scans all existing entries on its first iteration and therefore can raise events and collect data on its first iteration. On subsequent iterations, this script only scans the new entries that are written to the log file since the last monitoring interval. The default is n.
Include • error messages? • warning messages?	Set either of these parameters to **y** to collect error and warning messages. This script always returns informational messages related to canceled jobs.
Maximum threshold for canceled jobs	Enter the maximum number of canceled jobs allowed during any monitoring interval before an event is raised. The default is 10 canceled jobs.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

DeleteJobs

Use this Knowledge Script to delete all jobs or specific types of jobs from the ARCserve job queue. An event is raised if any jobs are successfully deleted. The event detail message reports the number of jobs actually deleted and also indicates when some jobs could not be deleted.

Note
If both ARCserve and ARCserveIT are installed on the same computer, only the ARCserveIT jobs are deleted.

Resource Objects

ARCserve server, ARCserveIT server

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event when job is successful?	Set this parameter to **y** to raise an event when the job succeeds. The default is n. **Note** This script always raises an event when the job fails.
Event severity level when job is successful	If you set the previous parameter to **y**, set the event severity level, from 1 to 40, to indicate the job ran successfully. The default severity level is 25 (blue event indicator). **Note** This script raises an event of severity 5 (red event indicator) when the job fails.
Collect data?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of jobs successfully deleted. The default is n.
Delete all jobs?	Set this parameter to **y** to delete all jobs in the ARCserve job queue. If set to **y**, any settings you select for the **Delete jobs of type** parameters are ignored. The default is n.
Delete jobs of type: • Backup • Restore • Copy • Count	If you disabled the **Delete all jobs** parameter, set any of these parameters to **y** to delete the jobs of that type. The default for each type of job is n.

EventLog

Use this Knowledge Script to periodically scan the Windows Application event log for entries created by ARCserve. The source label for these entries will be one of the following: `ARCserve`, `ARCserveIT`, or `CA_LIC`. If any ARCserve entries are found, an event is raised.

When this Knowledge Script starts, it uses the value specified for the **Start with events in past N hours** parameter to determine how to process entries already in the Application log. As it continues to run at the intervals specified on the **Schedule** tab, it scans the Application log for any new entries created since the last time it checked.

This Knowledge Script does not rely on a threshold to generate an event. When this Knowledge Script scans the Application log, it raises an event when it finds entries created by ARCserve. The event detail message returns the text of the ARCserve log entries found.

ARCserve Knowledge Scripts such as SuccessfulJobs and FailedJobs are available to monitor the most common ARCserve tasks. The EventLog Knowledge Script provides a flexible, general-purpose tool for monitoring other types of tasks or conditions that ARCserve Exec has written to the Application log. To fine-tune event log monitoring:

- Use the **Monitor events of type** parameters to scan only for certain types of events, such as Warning events.
- Use the **Filter the [...] field for** parameters to scan only for specific information, such as events with a specific ID.

Note

To use this Knowledge Script successfully, make sure ARCserve is configured to write event information to the Windows Application event log. You can use the SetLoggingType Knowledge Script to configure ARCserve to use the Application log. F

Resource Objects

ARCserve server, ARCserveIT server

Default Schedule

The default schedule is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of new event log entries. The default is n.

Description	How to Set It
Start with events in past N hours	Set this parameter to determine which events are included in the search the **first** time the Knowledge Script is run. Subsequent searches begin where the last search finished. The following entries are valid: • **-1** -- search all current and previous Application log events during the first monitoring interval. • **0** -- search only for events created since the last monitoring interval; previous events are not searched. • *N* -- search events logged in the past *N* hours to the Application log. For example, enter 8 to scan the last 8 hours of the Application log for matching entries. The default is 0.
Monitor for events of type: • Error • Warning • Information	Set to **y** for each type of event you want to monitor. If you disable any of these parameters, that type of entry does not raise an event, is not returned in an event detail message, and is not collected as data if you have enabled the **Collect data** parameter. The default is y.
Filter the [...] field for	To limit the types of log entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log: • **Event ID**. Specify a single ARCserve event ID or a range of event IDs separated by commas. For example: 1,2,10-15,202. • **Event Description**. Specify a description or keywords in the description. You can specify multiple descriptions separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Maximum number of entries per event message	Set the maximum number of Application log events that can be returned in each event report. For example, if this value is set to 30 and 67 Application log events are found, three event reports are created, two reports containing 30 events and one report containing 7 events. The **Message** column on the **Events** tab in the Operator Console or Control Center Console displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration. The default is 30 entries per event message.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. You may want to adjust the severity depending on which types of events you are checking for. The default severity level is 8 (red event indicator).

FailedJobs

Use this Knowledge Script to check for failed ARCserve jobs and to return data about those jobs.

This script periodically scans the latest ARCserve Activity log file (`ARCserve.log`) for entries that indicate a job failed. If the number of failed jobs found in the `ARCserve.log` file during any monitoring interval exceeds the threshold you set, an event is raised.

When an event is raised, the contents of the event detail message depend on whether you are also collecting data. When the Knowledge Script is collecting data, the event detail message reports the number of failed jobs. The data detail message contains the actual log entries. When the Knowledge Script is not collecting data, the event detail message returns all of the log entries related to failed jobs.

Note
If both ARCserve and ARCserveIT are installed on the same computer, only the ARCserveIT jobs are monitored.

Resource Objects

ARCserve server, ARCserveIT server

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of failed jobs. The default is n.
Start with new entries?	This parameter controls what the Knowledge Script does on its first iteration: • If set to **y**, this script does not scan existing entries on its first iteration, and therefore does not raise events or collect data on its first iteration. On subsequent iterations, this script only scans the new entries that were written to the log file since the last monitoring interval. • If set to n, this script scans all existing entries on its first iteration and therefore can raise events and collect data on its first iteration. On subsequent iterations, this script only scans the new entries that were written to the log file since the last monitoring interval. The default is n.
Include • error messages? • warning messages?	Set either of these parameters to **y** to scan error and warning messages. This script always returns informational messages related to canceled jobs.
Maximum threshold for failed jobs	Enter the maximum number of failed jobs allowed during any monitoring interval before an event is raised. The default is 10 failed jobs.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

HungJobs

Use this Knowledge Script to check for backup jobs that started but did not finish.

Use the **Expected duration of a job** parameter to specify the maximum amount of time, in minutes, that any single job can take to complete. This script periodically scans the latest ARCserve Activity log file (`ARCserve.log`) and makes a note of the start time of each job it finds. Any job that starts and then does not finish by the time you set as the expected duration considered "hung." If you set a threshold for the number of hung jobs, the script raises an event if the number of hung jobs exceeds this threshold. You can specify a threshold of 0 to receive an event when any job is hung.

Note
A job that has finished did not necessarily complete successfully. A job might have failed or have been canceled before the expected duration elapsed. Therefore, HungJobs is not a substitute for the monitoring provided by other ARCserve Knowledge Scripts, such as FaFailedJobsnd CaCanceledJobs.

If both ARCserve and ARCserveIT are installed on the same computer, only the ARCserveIT jobs are monitored.

Resource Objects

ARCserve server, ARCserveIT server

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of hung jobs. The default is n.
Start with new entries?	This parameter controls what the Knowledge Script does on its first iteration: • If set to **y**, this script does not scan existing entries on its first iteration, and therefore does not raise events or collect data on its first iteration. On subsequent iterations, this script only scans the new entries that were written to the log file since the last monitoring interval. • If set to n, this script scans all existing entries on its first iteration and therefore can raise events and collect data on its first iteration. On subsequent iterations, this script only scans the new entries that are written to the log file since the last monitoring interval. The default is n.
Jobs to monitor [separated by comma w/o space]	Specify the job ID of the backup job or jobs you want to monitor. Separate multiple job IDs with commas; leave this parameter blank to monitor all backup jobs.

Description	How to Set It
Expected duration of a job	Enter the maximum amount of time that any single job can take to complete. A job that does not complete within this expected duration is considered “hung.” The default is 30 minutes.
Maximum threshold for hung jobs	Enter the maximum number of hung jobs allowed before an event is raised. The default is 10 hung jobs.
Maximum number of jobs to monitor	Enter the maximum number of jobs that this Knowledge Script keeps track of at any given moment. By entering as small a number as is practical for your environment, you can fine-tune the amount of system resources that this script consumes. However, if the script reaches the maximum number of jobs, it will not keep track of any new jobs that start. Specify a value that is at least equal to or greater than the threshold you set. The default is 100 jobs.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

IncompleteJobs

Use this Knowledge Script to check for incomplete ARCserve jobs and to return data about those jobs.

This script periodically scans the latest ARCserve Activity log file (`ARCserve.log`) for entries that indicate a job was incomplete. If, during any interval, the number of incomplete jobs found in the `ARCserve.log` file is greater than the threshold you set, an event is raised.

When an event is raised, the contents of the event detail message depend on whether you are also collecting data. When the Knowledge Script is collecting data, the event detail message reports the number of incomplete jobs. The data detail message contains the actual log entries. When the Knowledge Script is not collecting data, the event detail message returns all of the log entries related to incomplete jobs.

Note
If both ARCserve and ARCserveIT are installed on the same computer, only the ARCserveIT jobs are monitored.

Resource Objects

ARCserve server, ARCserveIT server

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of incomplete jobs. The default is n.
Start with new entries?	This parameter controls what the Knowledge Script does on its first iteration: • If set to **y**, this script does not scan existing entries on its first iteration, and therefore does not raise events or collect data on its first iteration. On subsequent iterations, this script only scans the new entries that were written to the log file since the last monitoring interval. • If set to n, this script scans all existing entries on its first iteration and therefore can raise events and collect data on its first iteration. On subsequent intervals, this script only scans the new entries that were written to the log file since the last monitoring interval. The default is n.
Include • error messages? • warning messages?	Set either of these parameters to **y** to collect error and warning messages. This script always returns informational messages related to canceled jobs.

Description	How to Set It
Maximum threshold for incomplete jobs	Enter the maximum number of incomplete jobs allowed during any monitoring interval before an event is raised. The default is 10 incomplete jobs.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

LogFiles

Use this Knowledge Script to monitor the number of log files ARCserve has generated in its `Log` directory and to delete old log files. If the number of log files found in the ARCserve `Log` directory during any monitoring interval exceeds the threshold you set, an event is raised.

Note
If both ARCserve and ARCserveIT are installed on the same computer, only the ARCserveIT Activity log files are monitored.

Resource Objects

ARCserve server, ARCserveIT server

Default Schedule

The default schedule is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, returns the number of log files found. The default is n.
Delete files that are X days old	Enter a number that indicates when to delete old log files. The age of a log file is calculated from its creation date. For example, you might enter 2 days. If this script runs at 3 p.m. on the 25th of the month, it deletes any log files that were created before 3 p.m. on the 23rd of the same month. If you do not want to delete log files, enter 0. The default is 0.
Maximum threshold for log files	Enter the maximum number of log files allowed during any monitoring interval before an event is raised. The default is 1000 log files.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

Report_ActivityLogSize

Use this ARCserve_Report script to generate a report about the size of the ARCserve Activity log. This report lets you aggregate data by the time period that is, minute, hour, or day, and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the ActivityLogSize Knowledge Script.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Data settings	Use the following parameters to define the statistical calculation applied to data, and which of the data is displayed.
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the aggregation interval • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the aggregation interval • **Close**: The last value for the aggregation interval • **Change**: The difference between the first and last values for the aggregation interval (close - open = change) • **Count**: The number of data points for the aggregation interval

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value that is, lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is **yes**.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is **yes**.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is **yes**.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.

Description	How to Set It
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is **yes**.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Report_CPUandMemoryUsage

Use this ARCserve_Report script to generate a report about the CPU and memory usage of ARCserve services. This report lets you aggregate data by the time period that is, minute, hour, or day, and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the ResourceHigh Knowledge Script.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend. The legend is a truncated form of the data stream legend visible in the Operator Console or Control Center Console. • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	Use the following parameters to define the statistical calculation applied to data, and which of the data is displayed.

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the aggregation interval • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the aggregation interval • **Close**: The last value for the aggregation interval • **Change**: The difference between the first and last values for the aggregation interval (close - open = change) • **Count**: The number of data points for the aggregation interval
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value that is, lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is **yes**.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is **yes**.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is **yes**.

Description	How to Set It
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click in the Value column, and click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Click in the Value column, and click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is **yes**.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Report_NumberofCanceledJobs

Use this ARCserve_Report script to generate a report about the number of canceled ARCserve jobs. This report lets you aggregate data by the time period that is, minute, hour, or day, and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the CanceledJobs Knowledge Script.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Data settings	Use the following parameters to define the statistical calculation applied to data, and which of the data is displayed.
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggreagation interval • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the aggregation interval • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the aggregation interval • **Close**: The last value for the aggregation interval • **Change**: The difference between the first and last values for the aggregation interval (close - open = change) • **Count**: The number of data points for the aggregation interval

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value that is, lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is **yes**.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is **yes**.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is **yes**.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.

Description	How to Set It
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is **yes**.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Report_NumberofFailedJobs

Use this ARCserve_Report script to generate a report about the number of failed ARCserve jobs. This report lets you aggregate data by the time period that is, minute, hour, or day, and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the FailedJobs Knowledge Script.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Data settings	Use the following parameters to define the statistical calculation applied to data, and which of the data is displayed.
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval (for example, the average value for 1 Hour) • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the aggregation interval • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the aggregation interval • **Close**: The last value for the aggregation interval • **Change**: The difference between the first and last values for the aggregation interval (close - open = change) • **Count**: The number of data points for the aggregation interval

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value that is, lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is **yes**.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is **yes**.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is **yes**.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.

Description	How to Set It
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is **yes**.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Report_NumberofIncompleteJobs

Use this ARCserve_Report script to generate a report about the number of incomplete ARCserve jobs. This report lets you aggregate data by the time period that is, minute, hour, or day, and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the IncompleteJobs Knowledge Script.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Data settings	Use the following parameters to define the statistical calculation applied to data, and which of the data is displayed.
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the aggregation interval • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the aggregation interval • **Close**: The last value for the aggregation interval • **Change**: The difference between the first and last values for the aggregation interval (close - open = change) • **Count**: The number of data points for the aggregation interval

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value that is, lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is **yes**.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is **yes**.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is **yes**.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.

Description	How to Set It
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is **yes**.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Report_NumberofSuccessfulJobs

Use this ARCserve_Report script to generate a report about the number of successful ARCserve jobs. This report lets you aggregate data by the time period that is, minute, hour, or day, and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the SuccessfulJobs Knowledge Script.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Data settings	Use the following parameters to define the statistical calculation applied to data, and which of the data is displayed.
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggreagation interval • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the aggregation interval • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the aggreagation interval • **Close**: The last value for the aggregation interval • **Change**: The difference between the first and last values for the aggregation interval (close - open = change) • **Count**: The number of data points for the aggregation interval

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value that is, lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is **yes**.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is **yes**.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is **yes**.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.

Description	How to Set It
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is **yes**.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

RescheduleJobs

Use this Knowledge Script to adjust the scheduled run time of all jobs in the ARCserve job queue. This script works on all jobs in the ARCserve job queue. An event is raised if the job fails and, optionally, if the job is successful.

Note
If both ARCserve and ARCserveIT are installed on the same computer, only the ARCserveIT jobs are rescheduled.

Resource Objects

ARCserve server, ARCserveIT server

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event when job is successful?	Set this parameter to **y** to raise an event when the job succeeds. The default is n. **Note** This script always raises an event when the job fails.
Event severity level when job is successful	If you set the previous parameter to **y**, set the event severity level, from 1 to 40, to indicate that the job ran successfully. The default severity level is 25 (blue event indicator). **Note** This script raises an event of severity 5 (red event indicator) when the job fails.
Collect data?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of jobs successfully rescheduled. The default is n.
Adjust all jobs by (+ / -)	Specify the number of minutes to adjust the script's run time: • To reschedule jobs to run earlier, specify a negative number of minutes. Precede the number with a minus sign (-). For example, enter -60. • To reschedule jobs to run later, specify a number of minutes. Do not use a plus sign (+). For example, enter 60. The default is 0 (no adjustment).

ResourceHigh

Use this Knowledge Script to monitor the CPU and memory utilization of the ARCserve services that were found on a managed client during discovery. Monitored ARCserve services include:

- Database engine, displayed as **ASDBEngine** in the TreeView
- Job engine **(ASJobEngine)**
- Tape engine **(ASTapeEngine)**
- Discovery server **(ASDiscoverySvc)**
- Message engine **(ASMsgEngine)**

If you change the number of ARCserve services running on a managed client, run the ARCserve_Discovery Knowledge Script on that computer again.

You can set two thresholds: one for maximum CPU time and one for maximum memory utilization. If the CPU or memory utilization of any service exceeds the thresholds you set, an event is raised.

Resource Objects

ARCserve server, ARCserveIT server, individual ARCserve services

Default Schedule

The default schedule is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the CPU usage and the memory usage for each service it is monitoring. The default is n.
CPU usage	Enter the maximum amount of CPU resources that you want any single ARCserve service to consume before an event is raised. The default is 60%.
Memory usage	Enter the maximum amount of memory that you want any single ARCserve service to consume before an event is raised. The default is 6 MB.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 8 (red event indicator).

ServiceDown

Use this Knowledge Script to monitor any ARCserve services that were found on a managed client during discovery. All of the following ARCserve services may be monitored:

- Database engine, displayed as **ASDBEngine** in the TreeView
- Job engine **(ASJobEngine)**
- Tape engine **(ASTapeEngine)**
- Discovery server **(ASDiscoverySvc)**
- Message engine **(ASMsgEngine)**

If you change the number of ARCserve services running on a managed client, run the ARCserve_Discovery Knowledge Script on that computer again.

This Knowledge Script does not rely on a threshold to raise events. If this Knowledge Script finds that any of the services it is monitoring is down, it raises an event. You can configure this Knowledge Script to automatically restart any service that is down.

Resource Objects

ARCserve server, ARCserveIT server, individual ARCserve services

Default Schedule

The default schedule is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the value 100 every time it finds a service is up and the value 0 every time it finds a service is down. This provides a way to report on the percentage of system up time in any given period. The default is n.
Auto-start service?	Set to **y** to automatically restart any service that is down. The default is y.
Severity when auto-start...	You can set the event severity level, from 1 to 40, to indicate the importance when auto-start: • **... fails**. Specify a value that indicates the service is down and AppManager could not restart it. The default is 5 (red event indicator). • **... succeeds**. Specify a value that indicates the service was down and AppManager successfully restarted it. The default is 25 (blue event indicator). • **... is set to n**. Specify a value to indicate the service is down and the restart parameter has been disabled. This default is 18 (yellow event indicator).

SetLoggingType

Use this Knowledge Script to configure ARCserve to write event information to the Windows Application event log. An event can be raised when the job succeeds.

The EventLog Knowledge Script provides a flexible, general-purpose tool for scanning the Windows Application log for entries written by ARCserve. However, before running the EventLog Knowledge Script, you must make sure ARCserve has been configured to write event information to the Windows Application event log.

You can use the SetLoggingType Knowledge Script to configure ARCserve to write event information to the Application log. Or if ARCserve is already using the Application log, you can use this Knowledge Script to configure ARCserve not to use the Application log.

Resource Object

ARCserveIT server

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event when job is successful?	Set this parameter to **y** to raise an event when the job succeeds. The default is n. **Note** This script always raises an event when the job fails.
Event severity level when job is successful	If you set the previous parameter to **y**, set the event severity level, from 1 to 40, to indicate that the job ran successfully. The default severity level for this parameter is 25 (blue event indicator). **Note** This script raises an event of severity 5 (red event indicator) when the job fails.
Configure ARCserve to use NT event log?	Set to **y** to configure ARCserve to write event information to the Windows Application event log. If ARCserve is already configured to use the Application log, set this parameter to n to configure ARCserve not to use the Application log. The default is y.

SuccessfulJobs

Use this Knowledge Script to check for the number of successful ARCserve jobs and to return data about those jobs.

This script periodically scans the latest ARCserve Activity log file (`ARCserve.log`) for entries that indicate a job succeeded. During the first script iteration, this Knowledge Script does not scan existing entries in the log, and therefore does not return any results. As it continues to run at the interval specified on the **Schedule** tab, this script scans the `ARCserve.log` file for any new entries created since the last monitoring interval.

If, during any monitoring interval, the number of successful jobs found in the `ARCserve.log` file falls below the threshold you specify, an event is raised.

Note
If both ARCserve and ARCserveIT are installed on the same computer, only the ARCserveIT jobs are monitored.

Resource Objects

ARCserve server, ARCserveIT server

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of successful jobs found. The default is n.
Minimum threshold for successful jobs	Specify the minimum number of successful jobs required during any interval to prevent an event from being raised. If the number of failed jobs is less than this threshold, an event is raised. The default is 10 successful.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

Chapter 11
ASYNC Knowledge Scripts

The ASYNC category provides Knowledge Scripts for monitoring Microsoft Windows servers for file changes, event log entries, and SNMP traps as these events occur. The ASYNC Knowledge Scripts run on an asynchronous schedule, which means that they run when a monitored event occurs to provide real-time feedback.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
FilesChanged	Monitors files for changes as they occur.
NTEventLog	Monitors Windows event logs for new entries matching the include and exclude criteria you define.
NTEventLogRx	Monitors Windows event logs for new entries matching the filter criteria you define using regular expressions.
SNMPTrap	Checks for incoming SNMP traps forwarded from NetIQ Trap Receiver.

Creating Filters with Regular Expressions

Some Knowledge Scripts enable you to use regular expressions to define include and exclude filters for pattern-matching against the text being evaluated. Depending on the Knowledge Script you are working with, you may be able to use regular expression include and exclude filters when you are setting job properties or you may be able to maintain your search criteria independent of the Knowledge Script parameters in a separate filter file. You may also be able to use regular expression modifiers to further refine your filtering.

For example, if your **include filter** is `replic.*` and you specify the modifier `i` to make the search case-insensitive, the regular expression contains the wildcard (`.`) and repeat (`*`) special characters, indicating you want to find strings that start with `replic` followed by any string of characters. Messages containing either `replication` or `replicated` are captured.

The format is the same for the exclude filter. For example, to find log entries that do not start with the string `success`, the exclude filter might look like this:

```
^success.*
```

If you are only searching for included strings, you can leave the exclude filter blank. If you want to retrieve all messages in the log in a given interval, you can specify `.*` for the include filter and leave the exclude filter blank.

Using Special Characters

The following special characters can be used in regular expressions:

Use This Character	For This Purpose
.	Wildcard for any one character
*	Repeat zero or more occurrences
^	Beginning of the line
\$	End of the line
\	Escape the next meta-character
|	Alternate matches
[ ]	Any character in the class set. You can specify individual characters or ranges.
( )	Grouping characters. For example, you can specify (a|b|c) to indicate a match with a, or b, or c.
+	Quantifier indicating one or more occurrences
?	Quantifier indicating zero or one occurrence
{*n*}	Quantifier indicating exactly *n* occurrence
\w	A word character (alphanumeric plus _)
\s	A white-space character
\d	A digit character

Using Regular Expression Modifiers

In addition to the special characters you can use in creating the regular expression, there are a number of modifiers that can be used to modify how pattern-matching is handled. Valid modifiers include:

Modifier	Description
c	Complements the search list
g	Matches globally as many times as possible
i	Makes the search case-insensitive
m	Treats the string as multiple lines
o	Interpolates variables only once
s	Treats the regular expression string as a single long line
x	Allows for regular expression extensions

For additional information about writing regular expressions, see your Perl documentation or other regular expression resources.

FilesChanged

Use this Knowledge Script to monitor files for changes to the current size, time stamp, and file attributes. This script raises an event if the size, time stamp, or attribute indicates the file has been modified.

Because this script checks the file properties rather than the file content, you can use this script with almost any file type.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Asynchronous**. Regardless of the schedule you select, once you start the Knowledge Script, its job status appears as **Running**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the size, time stamp, or attribute indicates the file has been modified. The default is y.
Collect data?	Set to **y** to collect data about file modifications. The default is n.

File path	Provide a valid directory path and filename to specify the file (or files) you want to monitor.
	To monitor more than one file with a similar name or to monitor the creation and deletion of a file, use pattern-matching characters to specify the filename. Use an asterisk (*) to match all characters and use a question mark (?) to match a single character. For example:
	`C:\NetIQ Corporation\Temp\NetIQ Corporation_Debug\Tomc\m?.*`
	matches the following files:
	`mo.log`
	`mo.log.bkup`
	`ms.log`
	`ms.log.bkup`
	To monitor all files in a directory (including new and deleted files), specify a directory path without a filename, for example, `C:\temp`.

Check file size?	Set to **y** to monitor the file's current size. The default is y.
Check file last write time?	Set to **y** to monitor the file's modification time stamp. The default is y.
Check file attribute?	Set to **y** to monitor the file's attributes. The default is y.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which file modifications are detected. The default is 8 (red event indicator).

NTEventLog

Use this Knowledge Script to scan specified Windows logs for entries that match the criteria you specify. You can filter the event log entries by event type and by specifying a combination of include and exclude strings for each event field. This script raises an event when a log entry matches all your filter criteria. All event log entries that match the filtering criteria are returned in the event detail message.

This script requires the Microsoft **EventLog** service to be running on the managed client computer.

When you run this script, only new entries that are written to the event log after you start the job are reported. This script does not re-scan the entire event log each time it runs.

On computers where the Security log is updated frequently, such as domain controller computers, consider using the NetIQ Security Manager product to securely and quickly consolidate Security logs with low impact to the server. For more information, visit the NetIQ Web site at http://www.netiq.com/products/sm/default.asp.

Note
To specify filters using regular expressions, use the NTEventLogRx Knowledge Script.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Asynchronous**. Regardless of the schedule you select, once you start the Knowledge Script, its job status appears as **Running**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event when a log entry matches the criteria you specify. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. When enabled, data collection returns information about log entries that match the criteria you specify. The default is n.
Collect data during Maintenance Mode?	Set to **y** to collect data even if the remote computer is in maintenance mode. The default is n.
Case-sensitive in all filters?	Set to **y** to make all filter statements for this Knowledge Script case-sensitive. The default is n.
Event logs to filter (System, Security, DNS Server, Application)	Specify the names of the Windows event logs you want to filter, separating each log name with a comma. For example, on a Windows 2000 managed client computer, you might specify the following logs: `Security,DNS Server,Application` The default value, `Null`, filters all logs.

Parameter	How to Set It
Filter error events?	Set to **y** to filter error events. The default is y.
Filter warning events?	Set to **y** to filter warning events. The default is y.
Filter information events?	Set to **y** to filter information events. The default is y.
Filter success audit events?	Set to **y** to filter success audit events. The default is y.
Filter failure audit events?	Set to **y** to filter failure audit events. The default is y.
Filter events by source	To filter events generated by a particular source (for example `SQLExecutive`, `SNMP`, or `Service Control Manager`), enter an appropriate filter string. This script looks for matching entries in the event log's **Source** field. Multiple strings can be entered separated by commas. The default value, `Null`, filters log entries from all sources. The filter string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.
Filter events by category	To filter events in a particular category (for example Server or Logon), enter an appropriate filter string. This script looks for matching entries in the event log's **Category** field. Multiple strings can be entered separated by commas. The default value, `Null`, filters log entries from all categories. The filter string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.
Filter events by event ID	To filter events in a particular event ID, enter an appropriate filter string. This script looks for matching entries in the event log's **Event** field. Multiple IDs can be entered separated by commas. For example: `1,2,10,202` The default value, `Null`, filters log entries for all event IDs. The filter string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.
Filter events by user	To filter events associated with a particular user, enter a filter string that includes the user's domain name and user name, separated with a backslash "\". For example, `NetIQ Corporation\Tom Jones`. This script looks for matching entries as they appear in the **User** field of the event log's Event Detail dialog box (To view the Event Details dialog box, double-click a log entry in the Event Viewer). Separate multiple strings with commas (,). The default value, `Null`, filters log entries for all users. The filter string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.
Filter events by computer	To filter events generated by a particular computer, enter an appropriate filter string. This script looks for matching entries in the event log's **Computer** field. Multiple strings can be entered separated by commas. The default value, `Null`, filters log entries generated by all computers. The filter string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.

Parameter	How to Set It
Filter events by event description	To filter events with a particular detail description or containing keywords in the description, enter an appropriate filter string. This script looks for matching entries in the event log's **Description** field. Multiple strings can be entered separated by commas. The default value, `Null`, filters all log entry descriptions. The filter string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.
Severity for error events	Set the event severity level, from 1 to 40, to indicate the importance of an event in which error events are detected. The default is 5 (red event indicator).
Severity for warning events	Set the event severity level, from 1 to 40, to indicate the importance of an event in which warning events are detected. The default is 15 (yellow event indicator).
Severity for information events	Set the event severity level, from 1 to 40, to indicate the importance of an event in which information events are detected. The default is 25 (blue event indicator).
Severity for success audit events	Set the event severity level, from 1 to 40, to indicate the importance of an event in which success audit events are detected. The default is 5 (red event indicator).
Severity for failure audit events	Set the event severity level, from 1 to 40, to indicate the importance of an event in which failure audit events are detected. The default is 5 (red event indicator).

NTEventLogRx

Use this Knowledge Script to scan specified Windows logs for entries that match the criteria you specify. You can filter the event log entries by event type and by specifying a combination of include and exclude strings for each event field using regular expressions. This script raises an event when a log entry matches all your filter criteria. All event log entries that match the filtering criteria are returned in the event detail message.

Use the *Filter the [...] field with* parameters to control which fields to filter and the filtering criteria to use to find specific information, such as events associated with a specific user or computer name. With this script, specify the filtering criteria for each field you are interested in using a regular expression, or specify the name of a file that contains all your filtering criteria.

For more information, see "Creating Filters with Regular Expressions" on page 436.

Once you start the Knowledge Script job, any new entries written to the event log that match your criteria are reported. This script does not scan the entire log for any previously-reported events.

This scripts requires the Microsoft **EventLog** service to be running on the managed client computer.

On computers where the Security log is updated frequently, such as domain controller computers, consider using the NetIQ Security Manager product to securely and quickly consolidate Security logs with low impact to the server. For more information, visit the NetIQ Web site at http://www.netiq.com/products/sm/default.asp.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Asynchronous**. Regardless of the schedule you select, once you start the Knowledge Script, its job status appears as **Running**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event when a log entry matches the criteria you specify. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. When enabled, data collection returns information about log entries that match the criteria you specify. The default is n.
Make filters case-sensitive?	Set to **y** to make all filter statements for this script case-sensitive. The default is n.

Parameter	How to Set It
Event logs to filter for entries	Specify the names of the Windows event logs you want to filter, separating each log name with a pipe character (|). For example, on a Windows 2000 managed client computer, you might specify: `Security|System|Application` When this field is empty (the default value), the script filters all logs.
Filter the [...] field using the regular expression	Use a regular expression to indicate the criteria to look for in each event log field you are interested in: • **Type**. To filter information based on the type of event (such as Error, Warning, Information, Success Audit, Failure Audit), use a regular expression to identify the type of event entries to include. • **Source**. To filter the entries generated by a particular source (such as `SQLExecutive`, `SNMP`, or `Service Control Manager`), use a regular expression to identify the source of event entries to include. • **Category**. To filter information based on a particular category (such as Server or Logon), use a regular expression to identify the category of event entries to include. • **Event ID**. To filter information based on the event ID, use a regular expression to identify the event IDs to include. • **User**. To filter information based on the user name, use a regular expression to identify the user names to include. • **Computer**. To filter information based on the computer name, use a regular expression to identify the computers to include. • **Description**. To filter information based on the event description, use a regular expression to indicate the description to include.
Full path to a file containing filtering criteria	To specify matching expressions in an external file, type the full path to a file containing the filtering criteria you want to match. For example: `C:\TEMP\MyFilters.txt`. **Note** If you specify a filter file, AppManager ignores the *Filter the [...] field with* parameters. However, if AppManager cannot process the filter file, the script raises an event (for example, `fail to process filter file C:\async.xml`) and continues to scan the log files using the filtering criteria you specified in the *Filter the [...] field with* parameters. For more information, see "Using an External Filter File" on page 444.
Severity for error events	Set the event severity level, from 1 to 40, to indicate the importance of an event in which error events are detected. The default is 5 (red event indicator).
Severity for warning events	Set the event severity level, from 1 to 40, to indicate the importance of an event in which warning events are detected. The default is 15 (yellow event indicator).
Severity for information events	Set the event severity level, from 1 to 40, to indicate the importance of an event in which information events are detected. The default is 25 (blue event indicator).
Severity for success audit events	Set the event severity level, from 1 to 40, to indicate the importance of an event in which success audit events are detected. The default is 5 (red event indicator).

Parameter	How to Set It
Severity for failure audit events	Set the event severity level, from 1 to 40, to indicate the importance of an event in which failure audit events are detected. The default is 5 (red event indicator).
Severity for event filtering errors	Set the event severity level, from 1 to 40, to indicate the importance of an event in which filtering errors occurred. The default is 20 (yellow event indicator).

Using an External Filter File

Use this Knowledge Script to specify regular expressions for each event log field as script properties or maintain your search criteria independent of the script parameters in a separate filter file.

In many cases, specifying an external filter file provides greater flexibility and makes modifying your search criteria more straightforward, because you can add almost any number of expressions. You do not need to modify the script properties through the Operator Console or Control Center to pick up your changes.

To use a filter file:

- Identify the strings that you want to find a match for (that is, the entries you want to include in your results).
- Create a text file with one regular expression string per line to locate matching strings. Each line in the file consists of a parameter keyword followed by a colon (:), a tab or blank space, and the regular expression. Or the filter file can be written in XML.
- Ensure the file exists on the target computer.
- Provide the absolute path to the file on the local computer in the *Full path to a file containing filtering criteria* parameter and start the job.

Formatting the Filter File

There are two valid formats for the filter file: a simple table format to define the strings to include, and an XML format that allows you to define more complex include and exclude filtering. For both formats, the parameter name keywords are required, but the field values can be left blank if no filtering is needed.

Select a file format appropriate for the complexity of the filtering you need to do.

Table Format

The table format provides a simple way to create the filter file. Each filtering section in the file begins with `EventStart` and ends with `EventEnd`. If an entry in the event log matches all the criteria you specified within a filtering section, it is considered a match and an event is raised in AppManager. If you have more than one filtering section, an entry matching either section raises an event.

For example, the following table format file provides two filter sections:

```
EventStart
CaseSensitive:n
Log:System
Type:Error|Warning|Information
Source:^SQL*
Category:*
EVENTID:1[0-9][0-9][0-9]
User:Sam|Joe|Chris
Computer:SFO*
Description:($Error.*)|(.*error.*occurred.$)
```

```
EventEnd
EventStart
CaseSensitive:n
Log:Application
Type:Error|Warning|Information
Source:^SQL*
Category:*
EVENTID:1[0-9][0-9][0-9]
User:Sam|Joe|Chris
Computer:SFO*
Description:($Error.*)|(.*error.*occurred.$)
EventEnd
```

Note
If you specify only one filter section, do not include the EventStart and EventEnd lines in the file.

XML Format

The XML format is somewhat more sophisticated and more flexible than the table format. The XML format allows you to set both include and exclude filters using the `<Include>` and `<Exclude>` tags and to combine these filter sets to define the search criteria. Each filtering section in the file begins with the `<Events>` tag. An log entry must match all the criteria you specified within a filtering section for it to be considered a match.

For example:

```
<?xml version = "1.0" standalone = "yes"?>
<EventLogConfig Name = "Event Filter" Type = "EVENT_FILTER_CUSTOM" ID = "76">
<Include>
   <Events>
      <Log>Application</Log>
      <Type>INFORMATION|WARNING|ERROR</Type>
      <Source><Net*]></Source>
      <Category>*</Category>
      <EVENTID>2*</EVENTID>
      <User>*</User>
      <Computer>*</Computer>
      <Description><![CDATA[Event.]]></Description>
      <CaseSensitive>y</CaseSensitive>
   </Events>
   <Events>
      <Log>System</Log>
      <Type>Warning</Type>
      <Source>RSVP</Source>
      <Category>*</Category>
      <EVENTID>*</EVENTID>
      <User>*</User>
      <Computer>SHASTA</Computer>
      <Description>RSVP*</Description>
      <CaseSensitive>y</CaseSensitive>
   </Events>
</Include>
</EventLogConfig>
```

Note
If a field contains a regular expression that conflicts with XML syntax or includes special characters, you can use `![CDATA[regular_expression]]` to enclose the expression and prevent parsing problems.

SNMPTrap

Use this Knowledge Script to check for SNMP traps forwarded from NetIQ Trap Receiver (Trap Receiver). This script raises an event when an SNMP trap is received and when Trap Receiver is unavailable or subsequently becomes available. In addition, this script generates data streams for Trap Receiver availability. For more information, see "Working with NetIQ Trap Receiver" on page 449.

Prerequisites

- Trap Receiver is not installed automatically when you install the AppManager for Microsoft Windows module. You must start Trap Receiver manually by running the following:

  ```
  \AppManager\bin\NetIQTrapReceiver_Setup.exe
  ```

- This script supports SNMP v1, v2, and v3. If you use SNMP v3, configure your SNMP permissions in AppManager Security Manager. For more information, see "Configuring SNMP Permissions" on page 451.
- Trap Receiver filters SNMP traps based on the criteria you provide in the script parameters: IP address, hostname, or object identifier (OID). This script can translate numerical OIDs to their object descriptor (ODE) counterparts. The translation process requires access to the Management Information Base (MIB) files that reference the OIDs and ODEs. For more information, see "Adding MIBs for Use By Trap Receiver" on page 452.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Asynchronous**.

Setting Parameter Values

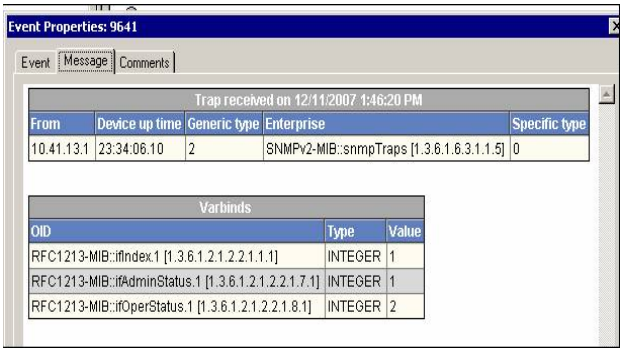
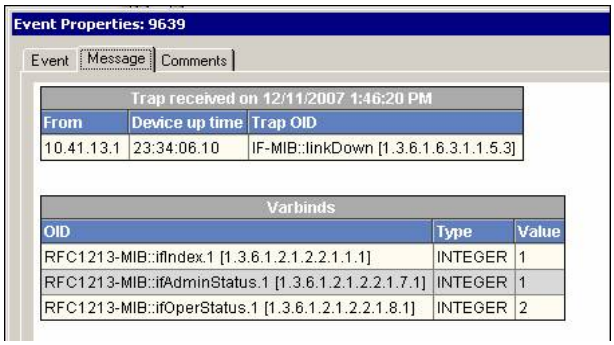
Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Error Notification	
Event severity when an error occurs	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMPTrap job fails. The default is 15. The default is 15.
Trap Filters	

Parameter	How to Set It
Filter by IP source address or hostname	Provide the IP address or hostname of the SNMP source from which to receive traps. For example: `10.10.10.10` Separate multiple addresses or hostnames with a comma (,). **Notes** • For SNMP v1 and v2, leave this parameter blank (the default) to receive traps from any source IP address or hostname. • For SNMP v3, you must provide at least one IP address or hostname from which to receive traps. Trap Receiver can receive traps only from devices that are registered in `net-snmp` with the appropriate profile information: username, security mode, and passwords.

Filter by object identifier	Provide the object identifier of the trap messages you want to receive. The object identifier is defined by the SNMP source agent.
	You can use OID or ODE notation to specify the object identifier. To filter for more than one object identifier, separate each notation with a comma (,).
	If you leave this parameter blank, the script does not use the object identifier to filter for events.
	If you are using ODE notation, use a case-sensitive descriptor. For example:
	`system.sysUptime.0`
	If you are using OID notation, include the dot (.) at the beginning of the identifier. For example:
	`.1.2.6.1.4.1.1691`
	Note This script filters for an exact match to the OID you provide. If your OID is `.1.2.6.1.4.1.1691`, the script will not match all OIDs that begin with `.1.2.6`. It matches only the OID you specified.

Filter by generic trap number	Specify a generic trap number to filter trap messages that use the same OID for more than one trap message. You usually do not need to filter for generic trap message numbers if the OID is unique. The generic value of the OID is defined by the SNMP source agent. If you leave this parameter blank, the script does not use a generic value to filter for events.
Filter by specific trap number	Specify a specific trap number to filter trap messages that use the same OID for more than one trap message. You usually do not need to filter for specific trap message numbers if the OID is unique. The specific value of the OID is defined by the SNMP source agent. If you leave this parameter blank, the script does not use a specific value to filter for events.
Event Notification	
Raise event when SNMP trap received?	Select **Yes** to raise an event when an SNMP trap matching your filter criteria is received. The default is Yes.
Event severity when SNMP trap received	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a trap message matches all filter criteria. The default is 15. You can adjust the severity depending on which type of message you are checking for.

Parameter	How to Set It
Format trap data according to SNMP version	Select the version of SNMP whose formatting should be used for trap event messages. The data provided by each format is the same; only the layout is different. An event message in SNMPv1 format looks like this:  An event message in SMMP v2 format looks like this: 
Raise event for Trap Receiver availability?	Select **Yes** to raise an event when Trap Receiver becomes unavailable and when Trap Receiver becomes available once again. The default is Yes.
Event severity when Trap Receiver is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes unavailable. The default is 5.
Event severity when Trap Receiver becomes available	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes available. The default is 25.
Data Collection	
Collect data for received traps?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns information about received traps based on your search criteria. The default is unselected.
Collect data for Trap Receiver availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns “1” if Trap Receiver is available and “0” if Trap Receiver is unavailable. The default is unselected.
Interval for collecting Trap Receiver availability data	Specify the frequency with which the script collects Trap Receiver availability data. The default is every 5 minutes.

Working with NetIQ Trap Receiver

In general, a trap receiver is an application that receives traps from SNMP agents. Trap Receiver receives and filters SNMP traps, and then forwards the traps to AppManager. Trap Receiver runs as a service, `NetIQTrapReceiver.exe`, and may compete for port usage with any other trap receiver installed on the same computer.

What is NetIQ Trap Receiver?

At its most basic, a trap receiver is an application that receives traps from SNMP agents. Trap Receiver receives, filters, and forwards SNMP traps to AppManager. When you use Trap Receiver with the AppManager for Microsoft Windows module, the SNMPTrap Knowledge Script raises events when SNMP traps are received.

What is an SNMP Trap?

Simple Network Management Protocol (SNMP) is a protocol-based system used to manage devices on TCP/IP-based networks. From devices on which an SNMP agent resides, such as routers and switches, SNMP sends unsolicited notifications, called traps, to network administrators when thresholds for certain conditions are exceeded. These conditions are defined by the vendor in a device's Management Information Base (MIB). The network administrator sets the thresholds.

Traps are composed of Protocol Data Units (PDUs). Each PDU contains the following information, organized in various ways depending on the version of SNMP in use:

- SNMP version number
- Community name of the SNMP agent
- PDU type
- Enterprise OID (object identifier), a unique number that identifies an enterprise and its system objects in the MIB
- IP address of the SNMP agent
- Generic trap type: Cold start, Warm start, Link down, Link up, Authentication failure, Egp Neighbor Loss, and Enterprise
- Specific trap type. When the Generic trap type is set to "Enterprise," a specific trap type is included in the PDU. A specific trap is one that is unique or specific to an enterprise.
- Time the event occurred
- Varbind (variable binding), a sequence of two fields that contain the OID and a value

Understanding Trap Receiver Architecture

Trap Receiver operates on a Client-Server architecture: the *Server*—the stand-alone Trap Receiver application—receives, filters, and forwards SNMP traps to the *Client*—an application that receives traps, such as AppManager. The Server may receive traps from standard UDP port 162 or from any other configured port. The Client and the Server can reside on the same computer or on separate (proxy) computers.

Communication between Client and Server is implemented as XML messages over a TCP connection. Only one Server is allowed per computer, however, several Clients are allowed per computer. Clients that are registered to the same Server share the same TCP connection. The Server TCP port should be known to all potential Clients.

Understanding the Trap Receiver Configuration File

The configuration file for Trap Receiver, `NetIQTrapReceiver.conf`, identifies the UDP and TCP ports used by Trap Receiver: the UDP port is used for receiving traps; the TCP port is used for communicating with the Client, such as AppManager or another supported NetIQ application. The configuration file also identifies the level of logging you want to use and whether port forwarding is enabled.

By default, the configuration file is installed in `[`*`installation directory`*`]\config`, and has the following format:

```
#################################################################
#
# NetIQTrapReceiver.conf
#
# A configuration file for NetIQ Trap Receiver
#
#################################################################

#########################
# TCP port
# Syntax: tcp_port [port]
# E.g. : tcp_port 2735
#########################
tcp_port 2735

#########################
# UDP port
# Syntax: udp_port [port]
# E.g. : udp_port 162
#########################
udp_port 162

#########################
# Forwarding
# Syntax: forward [address]:[port] [v1]
# E.g. : forward 127.0.0.1:1000 v1
#########################

#########################
# Log level
# Syntax: log_level error|warning|info|debug|xml
# E.g. : log_level info
#########################
log_level debug
```

If the configuration file cannot be found, cannot be parsed, or does not contain one of the required values, Trap Receiver is initialized with the default configuration as shown above.

When changing values in the configuration file, take into account the following:

- If you change the TCP port number, stop all asynchronous Knowledge Script jobs associated with the modules that support Trap Receiver. Run the Discovery_NT Knowledge Script on all monitored devices to enable the devices to recognize the new TCP port number.
- If you change the UDP port number, also change the UDP port number configured on the devices that send traps to Trap Receiver.
- If another service uses port 2735 or port 162, Trap Receiver *will not start*. The Trap Receiver log file will contain different levels of messages, based on the log_level you choose. Either change the port numbers in the configuration file, stop the service that is using the default Trap Receiver port numbers, or forward the traps coming in to UDP port 162.

- To forward incoming traps to another trap receiver, such as Microsoft SNMP Trap Service, set the Forwarding values as follows:
  `forward [`*`IP address of other trap receiver`*`]:[`*`port number of other trap receiver`*`] [`*`SNMP version`*`]`.
  For example: `forward 10.40.40.25:167 v1`. By default, incoming traps are not forwarded. For more information, see "Coexisting with Microsoft SNMP Trap Service" on page 451.
- Restart Trap Receiver after any change to the configuration file. From Control Panel, double-click **Administrative Tools** and then double-click **Services**. Right-click **NetIQ Trap Receiver** and select **Restart**.

Coexisting with Microsoft SNMP Trap Service

Two trap receivers cannot be in use on the same computer while using the same standard UDP port (162). If NetIQ Trap Receiver and another trap receiver such as Microsoft SNMP Trap Service are installed on the same computer and both are receiving traps, then configure Trap Receiver to use the standard UDP port and to forward incoming traps (UDP forwarding) to the other trap receiver. For more information, see "Understanding the Trap Receiver Configuration File" on page 450.

Then, configure the other trap receiver to use a different, non-standard, UDP port that is not in use by another application. The following are instructions for configuring Microsoft SNMP Trap Service.

To configure Microsoft SNMP Trap Service to use another port:

1. Navigate to `c:\Windows\system32\drivers\etc`.
2. Open the **services** file.
3. In the row for `snmptrap`, change the value for **udp** from 162 to another port number that is not in use by any other application. Use the same port number you set as the forwarding port in the Trap Receiver configuration file. For more information, see "Understanding the Trap Receiver Configuration File" on page 450.
4. Save and close the **services** file.
5. Restart Windows SNMP Trap Service. In Control Panel, double-click **Administrative Tools** and then double-click **Services**. Right-click **SNMP Trap Service** and select **Restart**.

Tip

To see which ports are in use, run `netstat.exe` from a command prompt. Then select an available port as the port for the other trap receiver service.

Configuring SNMP Permissions

For each device you want to monitor for SNMP v3 traps, configure Simple Network Management Protocol (SNMP) information in AppManager Security Manager *before* you run the SNMPTrap Knowledge Script. You do not need to configure permissions for SNMP v1 or v2.

By configuring SNMP information, you provide AppManager the permission it needs to access the Management Information Bases (MIBs) on SNMP-enabled devices.

The AppManager for Microsoft Windows module supports the following modes for SNMP v3:

- No authentication; no privacy
- Authentication; no privacy
- Authentication and privacy

In addition, the module supports the following protocols for SNMP v3:

- MD5 (Message-Digest algorithm 5, an authentication protocol)
- SHA (Secure Hash Algorithm, an authentication protocol)
- DES (Data Encryption Standard, encryption protocol)

Your SNMP v3 implementation may support one or more combinations of mode and protocol. That combination dictates the type of information you configure in AppManager Security Manager: user name (or entity), context name, protocol name, and protocol passwords.

Configure SNMP information for each device you want to monitor. On the Custom tab in Security Manager, complete the following fields:

Field	Description
Label	`SNMPTrap`
Sub-label	Indicate whether the community string information will be used for a single device or for all devices: • *For a single device,* type the <*`device name`*>. • *For all devices*, type `default`.
Value 1	SNMP user name, or entity, configured for the device. All SNMP v3 modes require an entry in the **Value 1** field.
Value 2	Name of the context associated with the user name or entity you entered in the **Value 1** field. A context is a collection of SNMP information that is accessible by an entity. If possible, enter a context that provides access to all MIBS for a device. *If the device does not support context*, type an asterisk (`*`). All SNMP v3 modes require an entry in the **Value 2** field.
Value 3	Combination of protocol and password appropriate for the SNMP v3 mode you have implemented. • For *no authentication/no privacy mode*, leave the **Value 3** field blank. • For *authentication/no privacy mode*, type `md5` or `sha` and the password for the protocol, separating each entry with a comma. For example, type `md5,abcdef` • For *authentication/privacy mode*, type `md5` or `sha` and the associated password, and then type des and the associated password, separating each entry with a comma. For example, type `sha,hijklm,des,nopqrs`

Adding MIBs for Use By Trap Receiver

The SNMPTrap Knowledge Script can translate numerical OIDs to their ODE counterparts. The translation process requires access to the Management Information Base (MIB) files that reference the OIDs you specified as filters in the script parameters.

You must copy the necessary MIB files to the default MIBs directory on the computer on which NetIQ Trap Receiver is installed. After installing the MIBs, reload the MIBs directory so the new MIBs can be compiled for use by Trap Receiver.

To add MIBs to the MIB directory and reload the directory:

1. On the computer on which Trap Receiver is installed, copy all necessary MIB files to the default directory: `\Program Files\NetIQ\AppManager\bin\MIBs`. Ensure you copy MIB files for all your modules, not only the MIB files for the module with the trap definition.

2. On that same computer, restart the AppManager agent services: `NetIQmc` (NetIQ AppManager Client Resource Monitor) and `NetIQccm` (NetIQ AppManager Client Communication Manager). Restarting the services allows Trap Receiver to load the MIB files.

Chapter 12
AvayaCM Knowledge Scripts

AppManager for Avaya Communication Manager provides the following Knowledge Scripts for monitoring Communication Manager servers and resources. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AddMIB	Adds management information bases for monitoring by the SNMPTrap Knowledge Script.
AddPhone	Adds Avaya IP phones as objects in the TreeView pane.
Announcements	Monitors announcements for queued calls, dropped calls, and peak port usage.
AttendantCalls	Monitors the switch processing element (SPE) for answered calls, abandoned calls, calls on hold, queued calls, active time, and average answer time.
CallActivity	Monitors call activity on selected Communication Managers.
CallFailures	Monitors calls for abnormal causes of termination.
CallQuality	Monitors calls for quality metrics such as jitter, latency, packet loss, MOS (Mean Opinion Score), and R-Value.
CallQuery	Queries call detail records retrieved from Communication Manager and stored in the Avaya CM supplemental database.
CPU_Usage	Monitors a Communication Manager server for system management CPU usage, operating system CPU usage, call processing CPU usage, and available CPU.
ESS_Status	Monitors the registration status of an Enterprise Survivable Server (ESS).
H248GatewayStatus	Monitors H.248 media gateways for alarms and unavailable H.248 links.
HuntGroupUsage	Monitors hunt groups for answered calls, queued calls, abandoned calls, and average call wait time.
LSP_Status	Monitors the registration status of Local Survivable Processors (LSP).
PhoneConnectivity	Monitors disconnected registered phones for a Communication Manager and retains a history of the monitored phones in the Avaya CM supplemental database.
PhoneDeregistrations	Monitors phone deregistrations for a Communication Manager and retains a history of the monitored phones in the Avaya CM supplemental database.

Knowledge Script	What It Does
PhoneInventory	Creates an inventory of the phones configured in a Communication Manager cluster.
PhoneQuality	Collects real-time voice quality statistics for active calls on Avaya IP phones.
RegisteredResources	Monitors changes in the number of resources registered on a Communication Manager server.
RemovePhone	Removes Avaya IP phone objects from the TreeView pane.
RetrieveConfigData	Retrieves Communication Manager configuration data about stations and gateways and stores it in the Avaya CM supplemental database.
SecurityViolations	Monitors security violations for barrier codes, monitors calls that generated authorization code violations, and monitors calls that generated station security violations.
SetupSupplementalDB	Creates an Avaya CM supplemental database in which to store call detail records, disconnected phone information, and deregistered phone information.
SNMPTrap	Checks for incoming SNMP traps forwarded from NetIQ SNMP Trap Receiver.
SystemUptime	Monitors the number of hours a Communication Manager has been operational since its last reboot.
TrunkGroupUsage	Monitors trunk groups for busy time, calls queued and not queued, and out-of-service trunks.
Recommended Knowledge Script Group	Runs all recommended Knowledge Scripts at one time.

AddMIB

Use this Knowledge Script to add MIB (management information base) files to the MIB tree that is monitored by the SNMPTrap Knowledge Script. The MIB files should be `ASN.1` text files with `.txt` or `.my` file extensions. The MIB files should not be compiled MIB files.

With this script you can copy a MIB file from an arbitrary directory to the MIB tree located in the `<AppManager directory>\bin\MIBs` directory. And, by using the *Reload MIB tree?* parameter, you can reload all MIBs in the tree without restarting the AppManager agent. A restart of the AppManager agent automatically reloads the MIB tree.

Scenarios for using this script include the following examples:

In This Scenario	Set These Parameters
You want to add a MIB file to the MIB tree, but do not want the addition to take effect until after the next restart of the AppManager agent.	*Full path to MIB files* and *List of MIB files*: Provide location and name of MIB file you want to add. *Reload MIB tree?*: Set to **No** (unselected).
You manually copied a MIB file to the MIB directory and want to reload all MIBs in the directory.	*Full path to MIB files* and *List of MIB files*: Leave blank. *Reload MIB tree?*: Select **Yes**. *MIB reload timeout*: Set new timeout value or accept default of 10 seconds.
To fix compiler errors, you edited some MIBs in the MIB directory. Now you want to reload the MIBs to ensure the errors have been fixed.	*Full path to MIB files* and *List of MIB files*: Leave blank. *Reload MIB tree?*: Select **Yes**. *MIB reload timeout*: Set new timeout value or accept default of 10 seconds.

Resource Object

AvayaCM Trap Receiver object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Full path to MIB files	Specify the full path to the folder that contains the MIB files you want to install. The AppManager agent on the proxy agent computer must have network access to the location you specify.
List of MIB files	Provide a comma-separated list of the MIB files you want to install. The MIB files should be `ASN.1` text files with `.txt` or `.my` file extensions. The MIB files should not be compiled MIB files. The MIB files you specify must be located in the folder you identified in the *Full path to MIB files* parameter.
Reload MIB tree?	Select **Yes** to update the MIB tree.

Parameter	How to Set It
MIB reload timeout	Specify the length of time AppManager should attempt to update the MIB tree before timing out and raising a failure event. The default is 10 seconds.
Event Notification	
Raise event if installation and reloading of MIB tree succeeds?	Select **Yes** to raise an event if installation of the MIB files and reloading of the MIB tree succeeds. The default is Yes. **Note** Reloading of the MIB tree can be successful even if no new MIB files are installed. Reloading of the MIB tree can proceed even if you provide no MIB files in the *List of MIB files* or *Full path to list of MIB files* parameter.
Event severity when installation and reloading of MIB tree succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the installation of MIB files and the reloading of the MIB tree succeeds. The default is 25.
Raise event if reload MIB parser warnings received?	Select **Yes** to raise an event if warning messages are received during the reload process. The default is Yes. Warning scenarios include: • MIBs are installed successfully but the *Reload MIB tree?* parameter is not set to Yes. • Not all specified MIB files were loaded to the MIB tree.
Event severity when reload MIB parser warnings received	Set the severity level, from 1 to 40, to indicate the importance of an event in which warning messages are received during the reload process. The default is 15.
Raise event if installation and reloading of MIB tree fails?	Select **Yes** to raise an event if AppManager fails to install or reload the specified MIB files. The default is Yes. Failure scenarios include: • MIB reload timeout period expired. • Not all specified MIB files were installed.
Event severity when installation and reloading of MIB tree fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the installation or reloading of the MIB tree fails. The default is 10.
Raise event with the list of currently installed MIBs?	Select **Yes** to raise an informational event that provides a list of all MIBs installed in the MIB tree. The default is Yes.
Event severity for the list of currently installed MIBs	Set the severity level, from 1 to 40, to indicate the importance of an event that provides a list of all MIBs installed in the MIB tree. The default is 25.

AddPhone

Use this Knowledge Script to add Avaya IP phones as objects to be monitored. You must add a phone before you can monitor it with the PhoneQuality script. This script raises an event when phones are added or if phones cannot be added.

Resource Object

AvayaCM Station folder

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the AddPhone job. The default is 5.
Retrieve SNMP configuration data for these phones?	Select **Yes** to retrieve SNMP configuration data for these phones. The default is unchecked. If you select **Yes**, you can run the addPhone script without first running the RetrieveConfigData script. If you do not select **Yes**, you must run RetreiveConfigData before running AddPhone.
Configuration Settings	
List of phone extensions	Provide a list of the extension numbers of the Avaya phones that you want to monitor. You can type one extension, a list of extensions, or a list of extension ranges. Separate multiple extensions with a comma. For example: `20001-20040,30001-30050,40000` **Note** If you have many extension numbers, you can list the extensions in a separate file and then use the following parameter to access that file.

Full path to file with list of phone extensions	If you have many extensions to monitor, you can type the full path to a file that contains a list of the phone extensions. Each extension or range of extensions in the file should be on a separate line. For example:
	`20001-20040`
	`30001-30050`
	`40000`
	Because the file must be accessible from the AppManager agent, the path must be a local directory on the proxy computer or a UNC path.
	Important If you type a UNC path, then the `netiqmc` service must be running as a user that has access to the path.

Event Notification	
Raise event if all phones are added successfully?	Select **Yes** to raise an event if the specified phones are successfully added to the TreeView pane. The default is Yes.
Event severity when phones are added successfully	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the specified phones are added successfully. The default is 25.

Parameter	How to Set It
Raise event if configuration retrieval succeeds?	Select **Yes** to raise an event if the Knowledge Script successfully retrieved SNMP configuration information for these phones. The default is unselected.
Event severity when the configuration retrieval succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script successfully retrieved SNMP configuration information for these phones. The default is 25.

Announcements

Use this Knowledge Script to monitor announcements for queued calls, calls that dropped while in queue, and peak usage of announcement ports.

Choose whether to monitor specific announcements or the top *n* announcements. This script raises an event if a threshold is exceeded. In addition, this script generates datastreams for calls queued, calls dropped, and peak port usage.

Note
This script does not support Communication Manager version 3.1.

Resource Object

AvayaCM Announcement object

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Announcements job. The default is 5.
Select monitor type	Select one of the following monitoring options: • **Top-N** — select to monitor *n* announcements with the highest values for queued calls, dropped calls, or peak port usage. If you select this option, provide the value for *n* in the *Number of announcements to monitor* parameter. • **Comma-separated** — select to monitor specific announcements. If you select this option, provide a list of announcement extensions in the *Comma-separated list of announcements to monitor* parameter.
Number of announcements to monitor	Specify the number of announcements you want to monitor. The default is 5.
Comma-separated list of announcement extensions	Provide a list of the announcement extensions you want to monitor. You can provide individual extension numbers, a range of extension numbers, or a combination of both. For example: `20001-20020,20055,20100-20200` Separate each number or range with a comma.
Enable use of SNMP GETBulk requests?	By default, this parameter is enabled, allowing the Announcements Knowledge Script job to access Communication Manager MIBs using `GETNext` and `GETBulk` SNMP requests, as appropriate. Disable this parameter to allow the script to use only `GETNext` requests. Not all MIB tables are extensive enough to need a `GETBulk` request. A `GETBulk` request is faster, but more CPU-intensive than a `GETNext` request.

Parameter	How to Set It
Number of rows to request for each GETBulk operation	Specify the number of rows from the MIB table to return in a `GETBulk` request. The default is 10 rows. The number of rows determines how much faster MIB data is returned. If CPU usage is too high, you can reduce the number of rows per `GETBulk` request or disable the *Enable use of SNMP GETBulk requests?* parameter.
Interval to pause between GETBulk requests	Specify the number of milliseconds to wait between GETBulk requests. The default is 100 milliseconds. The amount of delay can help with managing CPU usage and speed of SNMP requests. For example, a one-row `GETBUlk` with a 100-millisecond delay between requests executes more slowly and uses less CPU than a `GETNext` request.
Monitor Calls Queued	
Event Notification	
Raise event if number of calls queued exceeds threshold?	Select **Yes** to raise an event if the number of calls in queue for an announcement exceeds the threshold you set. The default is Yes.
Threshold - Maximum calls queued	Specify the highest number of calls that can be in queue for an announcement before an event is raised. The default is 0 calls.
Event severity when number of calls queued exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of calls in queue for an announcement exceeds the threshold. The default is 15.
Data Collection	
Collect data for calls queued?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls in queue for an announcement during the monitoring period. The default is Yes.
Monitor Calls Dropped	
Event Notification	
Raise event if number of calls dropped exceeds threshold?	Select **Yes** to raise an event if the number of calls dropped while in queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum calls dropped	Specify the highest number of calls that can be dropped while in queue before an event is raised. The default is 0 calls.
Event severity when number of calls dropped exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of calls dropped while in queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for calls dropped?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls dropped while in queue during the monitoring period. The default is unselected.
Monitor Peak Ports Used	
Event Notification	
Raise event if peak number of ports used exceeds threshold?	Select **Yes** to raise an event if the number of ports in use simultaneously exceeds the threshold you set. The default is Yes.
Threshold - Maximum peak ports used	Specify the highest number of ports that can be in use simultaneously before an event is raised. The default is 12 ports.

Parameter	How to Set It
Event severity when peak number of ports used exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of ports in use simultaneously exceeds the threshold. The default is 15.
Data Collection	
Collect data for peak ports used?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the highest number of ports in use simultaneously during the monitoring period. The default is Yes.

AttendantCalls

Use this Knowledge Script to monitor an active switch processing element (SPE) for statistics related to call attendants. This script raises an event if a monitored value exceeds the threshold you set. In addition, this script generates datastreams for the following statistics:

- Answered calls
- Calls abandoned before being answered
- Calls abandoned while on hold
- Calls placed on hold
- Queued calls
- Number of minutes attendants are active
- Average call answer time

Resource Object

AvayaCM Active SPE object

Default Schedule

By default, this script runs every hour because the SNMP data it monitors is updated only once an hour. If you change the schedule to a shorter interval, you may receive SNMP request errors until the SNMP data is repopulated.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the AttendantCalls job. The default is 5.
Monitor Answered Calls	
Event Notification	
Raise event if number of answered calls exceeds threshold?	Select **Yes** to raise an event if the number of calls answered by attendants exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of answered calls	Specify the maximum number of calls that can be answered by attendants before an event is raised. The default is 100 calls.
Event severity when number of answered calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of answered calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of answered calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls answered by attendants during the monitoring period. The default is Yes.

Parameter	How to Set It
Monitor Calls Abandoned Before Answered	
Event Notification	
Raise event if number of calls abandoned before answered exceeds threshold?	Select **Yes** to raise an event if the number of abandoned calls exceeds the threshold you set. The default is Yes. A call is considered abandoned when the caller hangs up before the call is answered.
Threshold - Maximum number of calls abandoned before answered	Specify the maximum number of calls that can be abandoned before an event is raised. The default is 10 calls.
Event severity when number of calls abandoned before answered exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of abandoned calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for number of calls abandoned before answered?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were abandoned before being answered by an attendant. The default is unselected.
Monitor Calls Abandoned While on Hold	
Event Notification	
Raise event if number of calls abandoned while on hold exceeds threshold?	Select **Yes** to raise an event if the number of calls that were abandoned while on hold exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of calls abandoned while on hold	Specify the maximum number of on-hold calls that can be abandoned before an event is raised. The default is 10 calls.
Event severity when number of calls abandoned while on hold exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of calls that were abandoned while on hold exceeds the threshold. The default is 10.
Data Collection	
Collect data for number of calls abandoned before answered?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were abandoned before being answered by an attendant. The default is unselected.
Monitor Calls on Hold	
Event Notification	
Raise event if number of calls on hold exceeds threshold?	Select **Yes** to raise an event if the number of calls that were placed on hold exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of calls on hold	Specify the maximum number of calls that can be placed on hold before an event is raised. The default is 100 calls.
Event severity when number of calls on hold exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of calls that were placed on hold exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of calls on hold?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were placed on hold during the monitoring period. The default is Yes.
Monitor Queued Calls	

Parameter	How to Set It
Event Notification	
Raise event if number of queued calls exceeds threshold?	Select **Yes** to raise an event if the number of calls in queue for an available attendant exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of queued calls	Specify the maximum number of calls that can be in queue before an event is raised. The default is 100 calls.
Event severity when number of queued calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of calls in queue for an available attendant exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of queued calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls in queue during the monitoring period. The default is Yes.
Monitor Time Attendants are Active	
Event Notification	
Raise event if time attendants are active exceeds threshold?	Select **Yes** to raise an event if the number of minutes in which attendants are active (on a call) exceeds the threshold you set. The default is Yes.
Threshold - Maximum time attendants are active	Specify the maximum number of minutes attendants can be active before an event is raised. The default is 15 minutes.
Event severity when time attendants are active exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of minutes that attendants are active exceeds the threshold. The default is 15.
Data Collection	
Collect data for time attendants are active?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of minutes in which attendants were active during the monitoring period. The default is Yes.
Monitor Average Answer Time	
Event Notification	
Raise event if average answer time exceeds threshold?	Select **Yes** to raise an event if the average number of minutes that attendants take to answer calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum average answer time	Specify the highest average number of minutes it can take attendants to answer calls before an event is raised. The default is 5 minutes.
Event severity when answer time exceeds threshold	Select the event severity level, from 1 to 40, to indicate the importance of an event in which the average number of minutes it takes for attendants to answer calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for answer time?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average number of minutes that attendants took to answer calls during the monitoring period. The default is Yes.

CallActivity

Use this Knowledge Script to monitor call activity on selected Communication Managers. This script raises an event if a threshold is exceeded. In addition, this script generates datastreams for the number of active calls and the number of completed calls.

When you start the CallActivity Knowledge Script job, the managed object begins collecting call detail records (CDRs) to store in the Avaya CM supplemental database. After the CallActivity job stops, the managed object continues to collect CDRs. CDR collection stops within a time period equal to two intervals of the job, but never less than 4 minutes after the CallActivity job stops.

Prerequisite

Run SetupSupplementalDB to create the Avaya CM supplemental database.

Resource Object

AvayaCM Active SPE object

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CallActivity job. The default is 5.
Monitor Active Calls	
Event Notification	
Raise event if number of active calls exceeds threshold?	Select **Yes** to raise an event if the number of active calls exceeds the threshold you set. The default is Yes.
Threshold - Number of active calls	Specify the maximum number of calls that can be active before an event is raised. The default is 100 calls.
Event severity when number of active calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were active during the monitoring period. The default is Yes.
Monitor Completed Calls	
Event Notification	

Parameter	How to Set It
Raise event if number of completed calls exceeds threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold you set. The default is Yes.
Threshold - Number of completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 100 calls.
Event severity when number of completed calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were completed during the monitoring period. The default is Yes.

CallFailures

Use this Knowledge Script to monitor call detail records (CDRs) in the Avaya CM supplemental database for calls that terminated with abnormal condition codes. You can indicate which condition codes should not be considered abnormal. This script raises an event if the number of failed calls exceeds the threshold or if the supplemental database contains no records. In addition, this script generates datastreams for the number of failed calls.

When you start the CallFailures Knowledge Script job, the managed object begins collecting CDRs to store in the supplemental database. After the CallFailures job stops, the managed object continues to collect CDRs. CDR collection stops within a time period equal to two intervals of the job, but never less than 4 minutes after the CallFailures job stops.

The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the CDR tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in the CDR table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the CDR tables for calls that disconnected within the range you select in the *Select call disconnect time range* parameter. Select **Run once** on the Schedule tab to run this script in troubleshooting mode. However, the managed object does not collect CDRs unless this script is running, which could pose a problem should you want to troubleshoot a call that occurred 5 minutes ago, for example. Therefore, to perform troubleshooting as needed, run this script as a separate job with data collection and events disabled, and set the schedule to run every *n* minutes. By doing so, the supplemental database will always contain data you can use for troubleshooting.

Prerequisite

Run SetupSupplementalDB to create the Avaya CM supplemental database.

Condition Codes

The following table identifies all supported condition codes:

Condition Code	Description
0	An intraswitch call, which originates and terminates on the switch
1 (A)	An attendant-handled call or an attendant-assisted call, except conference calls
4 (D)	An extremely long call or a call with an extremely high message count TSC. An extremely long call is one that lasts for 10 or more hours. An extremely high message count TSC is 9999 or more messages. When a call exceeds 10 hours, the system creates a call record with this condition code and a duration of 9 hours, 59 minutes, and 1-9 tenths of a minute. The system creates a similar call record with this condition code after each succeeding 10-hour period. When the call terminates, the system creates a final call record with a different condition code that identifies the type of call.

Condition Code	Description
6 (E)	A call the system did not record because system resources were unavailable. The CDR record includes the time and the duration of the outage. The system generates this condition code for: • Calls that the system routes to the attendant • Calls that require the CDR feature to overwrite records • ISDN calls that are not completed at the far end, if the Q.931 message indicates the reason that the call was not completed. The system does not generate the condition code for ISDN calls that receive inband tones.
7 (G)	Calls that use the AAR or ARS feature.
8 (H)	Calls that are served on a delayed basis by the Ringback Queuing feature.
9 (I)	An incoming call, a tandem call, an incoming NCA-TSC call, or a tandem NCA-TSC call
A	An outgoing call
B	An adjunct-placed outgoing call
C (L)	A conference call For trunk CDR, the system create a separate call record, with this condition code, for each incoming or outgoing trunk that is used during the conference call. If you disable ITCS and OTCS, the system records the extension of the originator of the conference call. The system does not record any other extension. If you disable ITCS, and you administer the originator of the conference call to use Intraswitch CDR, the system generates a call with this condition code whenever the originator of the conference dials a nontrunk conference participant. If ITCS is active, and you do not administer the originator of the conference call to use Intraswitch CDR, the system generates a call with this condition code whenever the originator of the conference dials an intraswitch conference participant.
E (N)	A call that the system does not complete because the following facilities to complete the call are unavailable: • Outgoing calls - The trunks are busy and no queue exists. - The trunks are busy and the queue is full. • Incoming calls - The extension is busy. - The extension is unassigned. This condition code also identifies an ISDN Call By Call Service Selection call that is unsuccessful because of an administered trunk usage allocation plan. Incoming trunk calls to a busy telephone do not generate a CDR record.
F	A call that the system does not complete because of one of the following conditions: • The originator of the call has insufficient calling privileges. • An NSF mismatch occurs for an ISDN call. • An authorization mismatch occurs for a data call.
G	A call that the system terminates to a ringing station
H	Notes that the system abandoned a ring call
I	A call that the system terminates to a busy station
J	An incoming trunk call that is a new connection that uses Additional Network Feature-Path Replacement (ANF-PR) or DCS with Rerouting. For more information, see the *Administrator Guide for Avaya Communication Manager*.
K	An outgoing trunk call that is a new connection that uses ANF-PR or DCS with Rerouting. For more information, see the *Administrator Guide for Avaya Communication Manager*.

Condition Code	Description
M	An outgoing trunk call that the system disconnects because the call exceeds the time allowed.
T	CDR records for calls that meet the following conditions: • The **Condition Code 'T' for Redirected Calls?** field on the CDR System Parameters screen is set to **y**. • The incoming trunk group is direct inward dialing (DID). • The system automatically redirects an incoming call off of the server.

Resource Object

AvayaCM Active SPE object

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CallFailures job. The default is 5.
Include call details?	Select **Yes** to include call details in the events raised by this script. Leave this parameter unselected to suppress the following call details: • Condition Code • Calling Number • Called Number • Connect Time • Disconnect Time • Duration **Note** If you configured Communication Manager to use Agent ID numbers, an event will identify an Agent ID or gateway, rather than a called or calling phone extension.
Raise event if no records found?	Select **Yes** to raise an event if there are no CDRs to monitor. This does not mean there are no CDRs with abnormal condition codes. Instead, it means there are no CDRs at all. The default is unselected.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no CDRs were found. The default is 25.
Query Filters	No matter how many calls match the filters you select, an event displays only the first 50 calls.
Exclude these failure codes	Provide a comma-separated list of the condition codes you do not want to monitor.
Exclude these failure codes on zero duration calls only	Provide a comma-separated list of the condition codes you do not want to monitor, but only for calls that have a duration of zero.

Parameter	How to Set It
Include only these FRL codes	Provide a comma-separated list of the Facilities Restriction Level (FRL) codes you want to use as filters. Leave this field blank to include all FRL codes. For more information, see "Step 6 (Optional): Configuring CDR Parameters to Filter by FRL Codes" on page 19. **Note** To avoid an error message, run the SetupSupplementalDB Knowledge Script once before running this script. Also, set up FRL at the Avaya System Access Terminal (SAT) interface before running this script. Do not use FRL at the Avaya SAT interface with previous versions of this module.
Minimum duration	Set this parameter to filter out records whose call duration is less than the specified value. Accept the default of 0 to ignore the filter for minimum call duration.
Maximum duration	Set this parameter to filter out records whose call duration is greater than or equal to the specified value. Accept the default of 0 to ignore the filter for maximum call duration.
Calling phone number	Specify the number of the calling phone you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any calling phone number. **Note** If you configured Communication Manager to use Agent ID numbers, an event will identify the Agent ID or gateway associated with the *Calling phone number* you enter here.
Phone number connector	Set this parameter only if you specify both a *Calling phone number* and a *Called phone number*. Your selection indicates how the script will connect the two parameters: AND or OR. The default is AND.
Called phone number	Specify the number of the called phone you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any called phone number. **Note** If you configured Communication Manager to use Agent ID numbers, an event will identify the Agent ID or gateway associated with the *Called phone number* you enter here.
Troubleshooting	
Call disconnect time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **Note** This parameter is valid only when you select **Run once** on the Schedule tab.
Monitor Failed Calls	
Event Notification	
Raise event if number of failed calls exceeds threshold?	Select **Yes** to raise an event if the number of calls that failed with an abnormal condition code exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of failed calls	Specify the maximum number of calls that can fail before an event is raised. The default is 0 calls.
Event severity when number of failed calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of failed calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of failed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that failed with an abnormal condition code during the monitoring period. The default is unselected.

CallQuality

Use this Knowledge Script to monitor RTCP packets in the Avaya CM supplemental database for call quality statistics: jitter, latency, packet loss, MOS (Mean Opinion Score), and R-Value. This script raises an event if a monitored value exceeds or falls below a threshold. MOS and R-Value are computed only for calls that use one of the following codecs: G.711u, G.711a, or G.729.

Note
You can trigger NetIQ Vivinet Diagnostics to diagnose the problem indicated by an event in which the percentage lost data threshold is exceeded. For more information, see "Triggering Call and Phone Quality Diagnoses" on page 477.

When you start the CallQuality Knowledge Script job, the managed object begins collecting RTCP packets to store in the Avaya CM supplemental database. After the CallQuality job stops, the managed object continues to collect packets. Packet collection stops within a time period equal to two intervals of the job, but never less than 4 minutes after the CallQuality job stops.

The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the supplemental database tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in a table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the supplemental database for calls that disconnected within the range you select in the *Select call disconnect time range* parameter. Select **Run once** on the Schedule tab to run this script in troubleshooting mode. However, the managed object does not collect RTCP packets unless this script is running, which could pose a problem should you want to troubleshoot a call that occurred 5 minutes ago, for example. Therefore, to perform troubleshooting as needed, run this script as a separate job with data collection and events disabled, and set the schedule to run every *n* minutes. By doing so, the Avaya CM supplemental database will always contain data you can use for troubleshooting.

Understanding Datastreams and Threshold Events

This script generates datastreams for average MOS, R-Value, jitter, latency (one-way delay), and packet loss. These average values are based on data from each phone involved in calls that completed during the script's interval, which is, by default, every 5 minutes. For example, in a given call, the calling phone's jitter was 30 milliseconds and the called phone's jitter was 75 milliseconds. For this call, the datastream would be a calculated average of the jitter for both phones: 52.5 milliseconds.

This calculated average is below the default threshold value of 60 milliseconds. However, AppManager raises threshold events based on values for each phone in a call, not on the average value. Therefore, for this call, AppManager would raise one event based on the 75 milliseconds of jitter for the called phone.

Prerequisite

Run SetupSupplementalDB to create the Avaya CM supplemental database.

Resource Object

AvayaCM Active SPE object

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CallQuality job. The default is 5.
Include call details?	Select **Yes** to include call details in the events raised by this script. Leave this parameter unselected to suppress the following call details: • Caller and Called Average MOS • Caller and Called Average R-Value • Caller and Called Jitter • Caller and Called Latency • Caller and Called Lost Packets • Caller and Called Codec • Caller and Called Number • Connect Time • Disconnect Time • Duration **Note** If you configured Communication Manager to use Agent ID numbers, an event will identify an Agent ID or gateway, rather than a called or calling phone extension.
Raise event if no records found?	Select **Yes** to raise an event if there are no RTCP packets to monitor in the Avaya CM supplemental database. This does not mean there are no records with call quality data. It means there are no records at all. The default is unselected.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no RTCP packets were found. The default is 25.
Query Filters	No matter how many calls match the filters you select, an event displays only the first 50 calls.
Maximum table size	Specify the maximum number of detail rows to include in an event message. The default is 50 rows.
Minimum duration	Use this parameter to filter out records whose call duration is less than the value you specify. Accept the default of 0 seconds to ignore the filter for minimum duration.
Maximum duration	Use this parameter to filter out records whose call duration is greater than or equal to the value you specify. Accept the default of 0 seconds to ignore the filter for maximum duration.
Calling phone number	Specify the number of the calling phone you want to find in the supplemental database. Wildcard characters are acceptable. Leave this parameter blank to search for any calling phone number. **Note** If you configured Communication Manager to use Agent ID numbers, an event will identify the Agent ID or gateway associated with the *Calling phone number* you enter here.

Parameter	How to Set It
Phone number connector	Set this parameter only if you specify both a *Calling phone number* and a *Called phone number*. Your selection indicates how the script will connect the two parameters: AND or OR. The default is AND.
Called phone number	Specify the number of the called phone you want to find in the supplemental database. Wildcard characters are acceptable. Leave this parameter blank to search for any called phone number. **Note** If you configured Communication Manager to use Agent ID numbers, an event will identify the Agent ID or gateway associated with the *Called phone number* you enter here.
Troubleshooting	
Call disconnect time range	Select a range of time and dates in which the query should search for data in the supplemental database. • Select **Fixed Time** to select specific days and times that the query should begin and end. • Select **Sliding** to select a number of hours, days, months, or years in which to search. The query starts its search at the time the job runs, and goes back through the supplemental database for the number of units you select. The default is Fixed Time. **Note** This parameter is valid only when you select **Run once** on the Schedule tab.
Monitor Average MOS	
Event Notification	
Raise event if average MOS falls below threshold?	Select **Yes** to raise an event if the average MOS value falls below the threshold. The default is Yes.
Threshold - Average MOS	Specify the lowest average MOS value that must occur to prevent an event from being raised. The default is 3.60.
Event severity when average MOS falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average MOS value falls below the threshold. The default is 5.
Data Collection	
Collect data for average MOS?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average MOS value during the monitoring period. The default is unselected.
Monitor Average R-Value	
Event Notification	
Raise event if average R-Value falls below threshold?	Select **Yes** to raise an event if the average R-Value falls below the threshold. The default is Yes.
Threshold - Average R-Value	Specify the lowest average R-Value that must occur to prevent an event from being raised. The default is 70.
Event severity when average R-Value falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average R-Value falls below the threshold. The default is 5.
Data Collection	
Collect data for average R-Value?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average R-Value during the monitoring period. The default is unselected.
Monitor Average Jitter	
Event Notification	

Parameter	How to Set It
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if the jitter value exceeds the threshold. The default is Yes.
Threshold - Maximum jitter	Specify the highest average jitter value that can occur before an event is raised. The default is 60 milliseconds.
Event severity when jitter exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the jitter value exceeds the threshold. The default is 15.
Data Collection	
Collect data for jitter?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of jitter that occurred during the monitoring period. The default is unselected.
Monitor Average Latency	
Event Notification	
Raise event if latency exceeds threshold?	Select **Yes** to raise an event if the latency value exceeds the threshold. The default is Yes.
Threshold - Maximum latency	Specify the highest amount of average latency that can occur before an event is raised. The default is 400 milliseconds.
Event severity when latency exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the latency value exceeds the threshold. The default is 15.
Data Collection	
Collect data for latency?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of latency that occurred during the monitoring period. The default is unselected.
Monitor Average Packet Loss	
Event Notification	
Raise event if packet loss exceeds threshold?	Select **Yes** to raise an event if the packet loss value exceeds the threshold. The default is Yes.
Threshold - Maximum packet loss	Specify the highest percentage of average packet loss that can occur before an event is raised. The default is 1%.
Event severity when packet loss exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the packet loss value exceeds the threshold. The default is 15.
Data Collection	
Collect data for packet loss?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of packet loss that occurred during the monitoring period. The default is unselected.

Triggering Call and Phone Quality Diagnoses

You can use NetIQ Vivinet Diagnostics to diagnose problems identified by AvayaCM Knowledge Scripts.

Using the existing methodology of launching an Action script based on an event, AppManager can launch Action_DiagnoseVoIPQuality to trigger Vivinet Diagnostics to diagnose the problem for events raised by the following Knowledge Scripts:

- **AvayaCM_CallQuality** events trigger Vivinet Diagnostics to diagnose the problem when average MOS, average R-Value, average jitter, average latency, and average packet loss fall below or exceed their thresholds.
- **AvayaCM_PhoneQuality** events trigger Vivinet Diagnostics to diagnose the problem when MOS, R-Value, jitter, latency, and packet loss fall below or exceed their thresholds during the data collection interval.

The Action script runs by default only if Vivinet Diagnostics 2.3 or later is installed on the computer on which the script is running.

To trigger Vivinet Diagnostics:

1. When setting parameter values for the PhoneQuality or CallQuality scripts, click the **Actions** tab. Action_DiagnoseVoIPQuality is selected by default.
2. Click **Properties** and enter values for all parameters for the Action script. For more information about the parameter values, click **Help** on the Properties for Action_DiagnoseVoIPQuality dialog box.

For more information about Vivinet Diagnostics and call quality diagnoses, see the *User Guide for Vivinet Diagnostics* and the Help for the Action_DiagnoseVoIPQuality Knowledge Script.

CallQuery

Use this Knowledge Script to search for call detail records (CDRs) retrieved from Communication Manager and stored in the Avaya CM supplemental database. The search is based on query filters you select. This script raises an event if no CDRs are found or if the number of CDRs found exceeds the threshold you set. In addition, this script generates a datastream for the number of records found.

When you start the CallQuery Knowledge Script job, the managed object begins collecting CDRs to store in the Avaya CM supplemental database. After the CallQuery job stops, the managed object continues to collect CDRs. CDR collection stops within a time period equal to two intervals of the job, but never less than 4 minutes after the CallQuery job stops.

The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the CDR tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in the CDR table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the CDR tables for calls that disconnected within the range you select in the *Select call disconnect time range* parameter. Select **Run once** on the Schedule tab to run this script in troubleshooting mode. However, the managed object does not collect CDRs unless this script is running, which could pose a problem should you want to troubleshoot a call that occurred 5 minutes ago, for example. Therefore, to perform troubleshooting as needed, run this script as a separate job with data collection and events disabled, and set the schedule to run every *n* minutes. By doing so, the Avaya CM supplemental database will always contain data you can use for troubleshooting.

Prerequisite

Run SetupSupplementalDB to create the Avaya CM supplemental database.

Resource Object

AvayaCM Active SPE object

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CallQuery job. The default is 5.

Parameter	How to Set It
Include call details?	Select **Yes** to include call details in the events raised by this script. Leave this parameter unselected to suppress the following call details: • Condition Code • Calling Number • Called Number • Connect Time • Disconnect Time • Duration (seconds)
Raise event if no records found?	Select **Yes** to raise an event if there are no CDRs to monitor. This does not mean there are no CDRs with call quality data. It means there are no CDRs at all. The default is unselected.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no CDRs were found. The default is 25.
Query Filters	No matter how many calls match the filters you select, an event displays only the first 50 calls.
Maximum table size	Specify the maximum number of detail rows to include in an event message. The default is 50 rows.
Minimum duration	Set this parameter to filter out records whose call duration is less than the specified value. Accept the default of 0 to ignore the filter for minimum call duration.
Maximum duration	Set this parameter to filter out records whose call duration is greater than or equal to the specified value. Accept the default of 0 to ignore the filter for maximum call duration.
Calling phone number	Specify the number of the calling phone you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any calling phone number. **Note** If you configured Communication Manager to use Agent ID numbers, an event will identify the Agent ID or gateway associated with the *Calling phone number* you enter here.
Phone number connector	Set this parameter only if you specify both a *Calling phone number* and a *Called phone number*. Your selection indicates how the script will connect the two parameters: AND or OR. The default is AND.
Called phone number	Specify the number of the called phone you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any called phone number. **Note** If you configured Communication Manager to use Agent ID numbers, an event will identify the Agent ID or gateway associated with the *Called phone number* you enter here.
Troubleshooting	
Call disconnect time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **Note** This parameter is valid only when you select **Run once** on the Schedule tab.
Monitor Records Found	
Event Notification	
Raise event if number of records exceeds threshold?	Select **Yes** to raise an event if the number of CDRs found exceeds the threshold. The default is Yes.
Threshold - Maximum number of records	Specify the maximum number of CDRs that can be found before an event is raised. The default is 0 CDRs.

Parameter	How to Set It
Event severity when number of records exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of CDRs found exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of records?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of CDRs found during the monitoring period.

CPU_Usage

Use this Knowledge Script to monitor a Communication Manager server for system management CPU usage, operating system CPU usage, call-processing CPU usage, and available CPU. Note that "available CPU" is the amount of CPU that is available for high-priority tasks, including CPU allocated for low-priority tasks. "Available CPU" is not the amount of CPU that is left over after system management, operating system, and call processing take their shares. Therefore, the four CPU usage values provided by this script can total more than 100%.

This script raises events when values exceed or fall below thresholds that you set. In addition, this script generates datastreams for all monitored metrics.

Resource Object

AvayaCM Active SPE object

Default Schedule

By default, this script runs every 2 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CPU_Usage job. The default is 5.
Monitor Call Processing CPU Usage	
Event Notification	
Raise event if call processing CPU usage exceeds threshold?	Select **Yes** to raise an event if the percentage of CPU used by call processing exceeds the threshold you set. The default is Yes.
Threshold - Maximum call processing CPU usage	Specify the maximum amount of CPU that call processing can use before an event is raised. The default is 80%.
Event severity when call processing CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of CPU used by call processing exceeds the threshold. The default is 15.
Data Collection	
Collect data for call processing CPU usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of CPU used by call processing for the monitoring period. The default is Yes.
Monitor System Management CPU Usage	
Event Notification	
Raise event if system management CPU usage exceeds threshold?	Select **Yes** to raise an event if the percentage of CPU used by system management processes exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum system management CPU usage	Specify the maximum percentage of CPU that system management processes can use before an event is raised. The default is 20%.
Event severity when system management CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of CPU used by system management processes exceeds the threshold. The default is 15.
Data Collection	
Collect data for system management CPU usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of CPU used by system management processes for the monitoring period. The default is unselected.
Monitor Operating System CPU Usage	
Event Notification	
Raise event if operating system CPU usage exceeds threshold?	Select **Yes** to raise an event if the percentage of CPU used by operating system processes exceeds the threshold you set. The default is Yes.
Threshold - Maximum operating system CPU usage	Specify the maximum percentage of CPU that operating system processes can use before an event is raised. The default is 20%.
Event severity when operating system CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of CPU used by operating system processes exceeds the threshold. The default is 15.
Data Collection	
Collect data for operating system CPU usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of CPU used by operating system processes for the monitoring period. The default is unselected.
Monitor Available CPU	
Event Notification	
Raise event if available CPU falls below threshold?	Select **Yes** to raise an event if the percentage of CPU that is available for Communication Manager falls below the threshold you set. The default is Yes.
Threshold - Minimum available CPU	Specify the minimum amount of CPU that must be available for Communication Manager before an event is raised. The default is 20%.
Event severity when available CPU falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which available CPU falls below the threshold. The default is 15.
Data Collection	
Collect data for available CPU?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of available CPU for the monitoring period. The default is unselected.

ESS_Status

Use this Knowledge Script to monitor the registration status of an Avaya Enterprise Survivable Server (ESS). An ESS allows a media server to be used as a backup controller to protect Communication Manager against catastrophic failure.

This script raises an event if the server deregisters or reregisters. In addition, this script generates a data point for server registration status: 0 for deregistered and 1 for reregistered.

Resource Object

AvayaCM ESS object

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the ESS_Status job. The default is 5.
Monitor Registration Status	
Data Collection	
Collect data for registration status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns a 0 if the ESS deregisters and a 1 if the ESS reregisters. The default is unselected.
Event Notification	
Raise event if server deregisters?	Select **Yes** to raise an event if the ESS deregisters from Communication Manager. The default is Yes.
Event severity when server deregisters	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ESS deregisters from Communication Manager. The default is 15.
Raise event if server reregisters?	Select **Yes** to raise an event if the ESS reregisters with Communication Manager. The default is Yes.
Event severity when server reregisters	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ESS reregisters with Communication Manager. The default is 25.

H248GatewayStatus

Use this Knowledge Script to monitor the status of H.248 media gateways, including the following items:

- Major alarms
- Minor alarms
- Warning alarms
- Status of H.248 (server to gateway) link

This script raises an event if a threshold is exceeded. In addition, this script generates datastreams for each monitored value.

Resource Object

AvayaCM H.248 Media Gateway object

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the H248GatewayStatus job. The default is 5.
Monitor Major Alarms	
Event Notification	
Raise event if number of major alarms exceeds threshold?	Select **Yes** to raise an event if the number of major alarms exceeds the threshold you set. The default is Yes.
Threshold - Maximum major alarms	Specify the highest number of major alarms that can occur before an event is raised. The default is 1 alarm.
Event severity when number of major alarms exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of major alarms exceeds the threshold. The default is 5.
Data Collection	
Collect data for major alarms?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of major alarms that occurred during the monitoring period. The default is Yes.
Monitor Minor Alarms	
Event Notification	

Parameter	How to Set It
Raise event if number of minor alarms exceeds threshold?	Select **Yes** to raise an event if the number of minor alarms exceeds the threshold you set. The default is Yes.
Threshold - Maximum minor alarms	Specify the highest number of minor alarms that can occur before an event is raised. The default is 5 alarms.
Event severity when number of minor alarms exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of minor alarms exceeds the threshold. The default is 10.
Data Collection	
Collect data for minor alarms?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of minor alarms that occurred during the monitoring period. The default is Yes.
Monitor Warning Alarms	
Event Notification	
Raise event if number of warning alarms exceeds threshold?	Select **Yes** to raise an event if the number of warning alarms exceeds the threshold you set. The default is Yes.
Threshold - Maximum warning alarms	Specify the highest number of warning alarms that can occur before an event is raised. The default is 10 alarms.
Event severity when number of warning alarms exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of warning alarms exceeds the threshold. The default is 15.
Data Collection	
Collect data for warning alarms?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of warning alarms that occurred during the monitoring period. The default is unselected.
Monitor H.248 Link Status	
Event Notification	
Raise event if H.248 link is down?	Select **Yes** to raise an event if the H.248 link is unavailable. The default is Yes.
Event severity when H.248 link is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the H.248 link is unavailable.
Data Collection	
Collect data for link status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns 0 if the link is up or 1 if the link is down. The default is Yes.

HuntGroupUsage

Use this Knowledge Script to monitor the status of hunt groups. This script raises an event if a monitored value exceeds the threshold you set. In addition, this script generates datastreams for the following statistics:

- Number of answered calls
- Number of queued calls
- Number of abandoned calls
- Average call wait time

Resource Object

AvayaCM Hunt Group object

Default Schedule

By default, this script runs every hour because the SNMP data it monitors is updated only once an hour. If you change the schedule to a shorter interval, you may receive SNMP request errors until the SNMP data is repopulated.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the HuntGroupUsage job. The default is 5.
Monitor Answered Calls	
Event Notification	
Raise event if number of answered calls exceeds threshold?	Select **Yes** to raise an event if the number of calls answered in the hunt group exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of answered calls	Specify the highest number of calls that can be answered in the hunt group before an event is raised. The default is 100 calls.
Event severity when number of answered calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of calls answered in the hunt group exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of answered calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls answered in the hunt group during the monitoring period. The default is Yes.
Monitor Abandoned Calls	
Event Notification	

Parameter	How to Set It
Raise event if number of abandoned calls exceeds threshold?	Select **Yes** to raise an event if the number of calls abandoned in the hunt group exceeds the threshold you set. The default is Yes. A call is considered abandoned when the caller hangs up before the call is answered.
Threshold - Maximum number of abandoned calls	Specify the highest number of calls that can be abandoned before an event is raised. The default is 5 calls.
Event severity when number of abandoned calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of abandoned calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of abandoned calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were abandoned during the monitoring period. The default is unselected.
Monitor Queued Calls	
Event Notification	
Raise event if number of queued calls exceeds threshold?	Select **Yes** to raise an event if the number of calls in queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of queued calls	Specify the highest number of calls that can be in queue before an event is raised. The default is 100 calls.
Event severity when number of queued calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of calls in queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for queued calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were in queue during the monitoring period. The default is Yes.
Monitor Average Call Wait Time	
Event Notification	
Raise event if average call wait time exceeds threshold?	Select **Yes** to raise an event if the average amount of call wait time exceeds the threshold you set. The default is Yes. Call wait time is the amount of time a call waits before being answered.
Threshold - Maximum average call wait time	Specify the highest amount of average wait time that calls can experience before an event is raised. The default is 1 minute.
Event severity when average call wait time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average amount of call wait time exceeds the threshold. The default is 15.
Data Collection	
Collect data for average call wait time?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average amount of wait time that calls experienced during the monitoring period. The default is unselected.

LSP_Status

Use this Knowledge Script to monitor the registration status of an Avaya Local Survivable Processor (LSP). An LSP allows a media server to be a survivable call-processing server for remote and branch customer locations.

This script raises an event if the processor deregisters or reregisters. In addition, this script generates a data point for processor registration status: 0 for deregistered and 1 for reregistered.

Resource Object

AvayaCM LSP object

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the LSP_Status job. The default is 5.
Monitor Registration Status	
Data Collection	
Collect data for registration status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns a 0 if the LSP deregisters and a 1 if the LSP reregisters. The default is unselected.
Event Notification	
Raise event if processor deregisters?	Select **Yes** to raise an event if the LSP deregisters from Communication Manager. The default is Yes.
Event severity when processor deregisters	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the LSP deregisters from Communication Manager. The default is 15.
Raise event if processor reregisters?	Select **Yes** to raise an event if the LSP reregisters with Communication Manager The default is Yes.
Event severity when processor reregisters	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the LSP reregisters with Communication Manager. The default is 25.

PhoneConnectivity

Use this Knowledge Script to monitor disconnected registered phones for a Communication Manager and to maintain a history of the monitored phones in the Avaya CM supplemental database. This script raises an event if the number or percentage of disconnected registered phones exceeds the threshold you set. You can group events by cluster, building, floor, or type of phone.

Prerequisites

- Run SetupSupplementalDB to create the Avaya CM supplemental database.
- Run RetrieveConfigData to populate the Avaya CM supplemental database.

Resource Object

AvayaCM_ActiveSPE

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the PhoneConnectivity job. The default is 5.
Enable use of SNMP GETBulk requests?	By default, this parameter is enabled, allowing the PhoneConnectivity Knowledge Script job to access Communication Manager MIBs using `GETNext` and `GETBulk` SNMP requests, as appropriate. Disable this parameter to allow the script to use only `GETNext` requests. Not all MIB tables are extensive enough to need a `GETBulk` request. A `GETBulk` request is faster, but more CPU-intensive than `GETNext`.
Number of rows to request for each GETBulk operation	Specify the number of rows from the MIB table to return in a `GETBulk` request. The default is 10 rows. The number of rows determines how much faster MIB data is returned. If CPU usage is too high, you can reduce the number of rows per `GETBulk` or disable the *Enable use of SNMP GETBulk requests?* parameter.
Interval to pause between GETBulk requests	Specify the number of milliseconds to wait between GETBulk requests. The default is 100 milliseconds. The amount of delay can help manage CPU usage and speed of SNMP requests. For example, a one-row `GETBulk` with a 100-millisecond delay between requests runs more slowly and uses less CPU than a `GETNext` request.
Event Notification	

Parameter	How to Set It
Raise event if disconnected registered phones in group exceed threshold?	Select **Yes** to raise an event if the number or percentage of disconnected registered phones in a group exceeds the threshold you set. The default is Yes. Use *Type of threshold* to create a “number” or “percentage” event. Use *Select event grouping* to select how to group the deregistered phones.
Select event grouping	Select whether to group disconnected registered phones by **Cluster**, **Building**, **Floor,** or **Type** of phone. AppManager raises an event when the number or percentage of phones in *each* group exceeds the threshold you set. For example, suppose the following were true: • You set *Maximum number of disconnected registered phones in the group* to “5” • You set *Select event grouping* to “Building,” and you have three buildings. If AppManager detects six disconnected registered phones in the first building, two in the second, and seven in the third, it will raise two events: one for the six disconnected registered phones in the first building and another for the seven disconnected registered phones in the third building. Because you set the threshold to “5,” no event is raised for the disconnected registered phones in the second building. The default is Cluster.
Type of threshold	Select whether you want to raise events based on the **Number** or **Percent** of disconnected registered phones. The default is Number.
Threshold - Maximum number of disconnected registered phones	Use this parameter if you selected **Number** in *Type of threshold*. Specify the maximum number of registered phones that can be disconnected before an event is raised. The default is 0 phones.
Threshold - Maximum percent of disconnected registered phones	Use this parameter if you selected **Percent** in *Type of threshold*. Specify the maximum percentage of registered phones that can be disconnected before an event is raised. The default is 0%.
Event severity when disconnected registered phones exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number or percentage of disconnected registered phones in a group exceeds the threshold you set. The default is 15.
Include phone details in event message?	Select **Yes** to include details of the disconnected registered phones in the event message. Phone details can include station extension, station name, building, floor, station type, room, cable, jack, port, and deregistration time. The default is Yes.
Maximum number of detail rows to include in event message	Use this parameter if you selected **Yes** in *Include deregistered phone details in event message*. Specify the maximum number of detail rows to include in an event message. Each row contains details for one phone. Rows are sorted by most recently disconnected phone. Specify “0” to include all rows. The default is 20 rows.

PhoneDeregistrations

Use this Knowledge Script to monitor phone deregistrations for Communication Manager and to maintain deregistration history in the Avaya CM supplemental database. This script raises an event if the number or percentage of deregistered phones exceeds the threshold you set. You can group events by building, floor, or type of phone.

Prerequisites

- Run SetupSupplementalDB to create the Avaya CM supplemental database.
- Run RetrieveConfigData to populate the Avaya CM supplemental database.

Resource Object

AvayaCM Active SPE object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the PhoneDeregistrations job. The default is 5.
Enable use of SNMP GETBulk requests?	By default, this parameter is enabled, allowing the PhoneDeregistrations job to use `GETNext` and `GETBulk` SNMP requests to access Communication Manager MIBs. Disable this parameter to allow the script to use only `GETNext` requests. Not all MIB tables are extensive enough to need a `GETBulk` request. A `GETBulk` request is faster, but more CPU-intensive than `GETNext`.
Number of rows to request for each GETBulk operation	Specify the number of rows from the MIB table to return in a `GETBulk` request. The default is 10 rows. The number of rows determines how quickly MIB data is returned. If CPU usage is too high, you can reduce the number of rows per `GETBulk` or disable the *Enable use of SNMP GETBulk requests?* parameter.
Interval to pause between GETBulk operations	Specify the number of milliseconds to wait between GETBulk requests. The default is 100 milliseconds. The amount of delay can help with managing CPU usage and speed of SNMP requests. For example, a one-row `GETBulk` with a 100-millisecond delay between requests executes more slowly and uses less CPU than a `GETNext` request.
Event Notification	

Parameter	How to Set It
Raise event if deregistered phones in group exceed threshold?	Select **Yes** to raise an event if the number or percentage of deregistered phones in a group exceeds the threshold you set. The default is Yes. Use *Type of threshold* to create a “number” or “percentage” event. Use *Select event grouping* to select how to group the deregistered phones.
Select event grouping	Select whether to group deregistered phones by **Cluster**, **Building**, **Floor,** or **Type** of phone. AppManager raises an event when the number or percentage of deregistered phones in *each* group exceeds the threshold you set. For example, suppose the following were true: • You set *Maximum number of deregistered phones in the group* to “5.” • You set *Select event grouping* to “Building,” and you have three buildings. If AppManager detects six deregistered phones in the first building, two in the second, and seven in the third, it will raise two events: one for the six deregistered phones in the first building and another for the seven deregistered phones in the third building. Because you set the threshold to “5,” no event is raised for the deregistered phones in the second building. The default is Cluster.
Type of threshold	Select whether you want to raise events based on the **Number** or **Percent** of deregistered phones. The default is Number.
Threshold - Maximum number of deregistered phones	Use this parameter if you selected **Number** in *Type of threshold*. Specify the maximum number of phones that can be deregistered before an event is raised. The default is 0 phones.
Threshold - Maximum percent of deregistered phones	Use this parameter if you selected **Percent** in *Type of threshold*. Specify the maximum percentage of phones that can be deregistered before an event is raised. The default is 0%.
Event severity when deregistered phones exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number or percentage of deregistered phones in a group exceeds the threshold you set. The default is 15.
Include deregistered phone details in event message?	Select **Yes** to include details of the deregistered phones in the event message. Phone details can include station extension, station name, building, floor, station type, room, cable, jack, port, and deregistration time. The default is Yes.
Maximum number of detail rows to include in event message	Use this parameter if you selected **Yes** in *Include deregistered phone details in event message*. Specify the maximum number of detail rows to include in an event message. Each row contains details for one phone. Rows are sorted by most recently deregistered phone. Specify “0” to include all rows. The default is 20 rows.

PhoneInventory

Use this Knowledge Script to create an inventory of the phones configured in a Communication Manager cluster. You choose both the search criteria for the inventory and the location of the output folder for the results file containing the inventory list. Unless you specify a UNC path, *servername**sharename**directoryname**filename*, the results file is written to the computer on which the NetIQ AppManager agent is running. If you specify a UNC path, ensure the `NetIQmc` service is running as an account that has proper permissions on the UNC path.

Resource Object

AvayaCM Active SPE object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the PhoneInventory job. The default is 5.
Enable use of SNMP GETBulk requests?	By default, this parameter is enabled, allowing the PhoneInventory job to use `GETNext` and `GETBulk` SNMP requests to access Communication Manager MIBs. Disable this parameter to allow the script to use only `GETNext` requests. Not all MIB tables are extensive enough to need a `GETBulk` request. A `GETBulk` request is faster, but more CPU-intensive than `GETNext`.
Number of rows to request for each GETBulk operation	Specify the number of rows from the MIB table to return in a `GETBulk` request. The default is 10 rows. The number of rows determines how quickly MIB data is returned. If CPU usage is too high, you can reduce the number of rows per `GETBulk` or disable the *Enable use of SNMP GETBulk requests?* parameter.
Interval to pause between GETBulk operations	Specify the number of milliseconds to wait between GETBulk requests. The default is 100 milliseconds. The amount of delay can help with managing CPU usage and speed of SNMP requests. For example, a one row `GETBulk` with a 100-millisecond delay between requests executes more slowly and uses less CPU than a `GETNext` request.
Raise event if phone inventory succeeds?	Select **Yes** to raise an event when a phone inventory file is successfully generated. The default is Yes.

Parameter	How to Set It
Event severity when phone inventory succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an inventory file is successfully generated. The default is 25.
Raise event if no records found?	Select **Yes** to raise an event when the PhoneInventory job finds no phones based on the criteria you selected. The default is Yes.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the PhoneInventory job found no phones based on the criteria you selected. The default is 25.
Search Options	
Select by	Select the filter by which you want to create the list of phones. • Name • Extension (the default) • Building • Floor • Type
Selection criteria	Type the selection criteria for the phones to be listed. You can specify the actual item or you can specify a pattern by using the * wildcard. For example, to monitor all the phones in the ADM building, enter `ADM*`. You can enter multiple items by separating each item with a comma. For example: `ADM0009A*,ADM0009B*` The items you enter must be of the same type as the *Select by* parameter. So if *Select by* is Name, then the items you enter must be device names or patterns. If *Select by* is Extension, then the items you enter must be phone extension numbers. **Note** Only the following characters are acceptable in this parameter: • Number • Uppercase and lowercase letters • Periods • Commas • Asterisks (*) • Underscores • Spaces
List only phones with status of	To further filter the list of phones, select a status. Only phones with this status that also match the criteria you specified in *Selection criteria* and *Select by* will be included in the inventory list. Select from the following status types: • Any • Registered • Registered Not Connected • Unregistered
Result File Options	
Full path to output folder for result file	Type the full path or a UNC path to a location on the agent computer in which to save the inventory `.csv` file. The default path is `c:\Program Files\NetIQ\Temp\NetIQ_Debug\PhoneInventory.csv`
Order by	Select **Name** to display the contents of the results file in order by phone name. Select **Extension** to display the contents of the results file in order by phone extension number. The default is Extension.

PhoneQuality

Use this Knowledge Script to collect real-time voice-quality statistics for active calls on Avaya IP phones. This script raises one event per call if statistics exceed or fall below the thresholds you set. In addition, this script generates datastreams for the following statistics:

- Maximum interval MOS
- Maximum interval R-Value
  MOS and R-Value are computed only for calls that use one of the following codecs: G.711u, G.711a, or G.729.
- Maximum interval jitter
- Maximum interval latency
- Maximum interval packet loss

Note
You can trigger NetIQ Vivinet Diagnostics to diagnose the problem when voice quality thresholds are exceeded. For more information, see "Triggering Call and Phone Quality Diagnoses" on page 477.

When you start the PhoneQuality Knowledge Script job, the managed object begins collecting voice quality statistics. The managed object stops collecting statistics approximately one minute after the PhoneQuality job stops. If you attempt to delete a phone on which collection is still occurring, the following event is raised:

```
The phone(s) could not be removed because one or more phones are currently being
monitored by the PhoneQuality Knowledge Script. You must stop the PhoneQuality
job(s) before removing the phones.
```

Note
Unlike other proxy-based AppManager modules, AppManager for Avaya Communication Manager supports only one AppManager repository (`QDB`) per proxy agent computer. This limitation ensures the accuracy of monitoring phones with the PhoneQuality script. The list of phones for monitoring with this script does not differentiate between repositories; if multiple repositories were allowed, you could very well monitor the wrong set of phones for a given repository.

Prerequisite

Run AddPhone to add phones to be monitored. The PhoneQuality script is not available until after you run the AddPhone script.

Resource Object

AvayaCM Station object

Important
Do not monitor more than 100 active phone (station) objects in one cluster or across multiple clusters.

Default Schedule

By default, this script runs on an asynchronous schedule.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the PhoneQuality job. The default is 5.
Monitor Settings	
Data collection interval for voice quality metrics	Specify the interval at which data points are generated for voice quality metrics. The default is 30 seconds. The minimum is 15 seconds. **Note** Communication Manager sends RTCP packets to the proxy computer in almost real-time. If your data collection interval is the default, 30 seconds, and you are monitoring 100 phones and collecting data for only one metric, such as MOS, AppManager will generate about three data points per second (100 phones / 30 seconds). With all five metrics enabled, AppManager will generate about 16 data points per second. If you change to a more frequent data collection interval, for example every 15 seconds, AppManager will generate about 32 data points per second.
Additional fixed delay for MOS/R-Value calculation	Enter an amount of delay (in milliseconds) that you want to add to a call. This delay is in addition to the three other types of delay associated with calculating MOS and R-Value: • Network delay in one direction. • Packetization delay. This value is fixed, based on the type of codec being used. • Jitter buffer delay. This value is fixed, based on the type and size of the jitter buffer being used. The default is 0 milliseconds.
Monitor Interval MOS	
Event Notification	
Raise event if interval MOS falls below threshold?	Select **Yes** to raise an event if the value of interval MOS falls below the threshold that you set. The default is Yes. Interval MOS is the MOS value measured *during* the data collection interval you set. It is not the MOS value at the instance of data collection.
Threshold - Minimum interval MOS	Specify the lowest interval MOS value that can be calculated before an event is raised. The default is 3.60.
Event severity when interval MOS falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the interval MOS value falls below the threshold you set. The default is 5.
Data Collection	
Collect data for interval MOS?	Select **Yes** to collect interval MOS data for charts and graphs. When enabled, data collection returns the value of interval MOS measured during the data collection interval. The default is Yes.
Monitor Interval R-Value	
Event Notification	
Raise event if interval R-Value falls below threshold?	Select **Yes** to raise an event if interval R-Value falls below the threshold that you set. The default is Yes. Interval R-Value is the R-Value measured *during* the data collection interval you set. It is not the R-Value at the instance of data collection.

Description	How To Set It
Threshold - Minimum interval R-value	Enter the lowest interval R-Value that can be calculated before an event is raised. The default is 70.
Event severity when interval R-value falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which interval R-Value falls below the threshold you set. The default is 5.
Data Collection	
Collect data for interval R-Value?	Select **Yes** to collect interval R-Value data for charts and graphs. When enabled, data collection returns the value of interval R-Value measured during the data collection interval. The default is unselected.
Monitor Interval Jitter	
Event Notification	
Raise event if interval jitter exceeds threshold?	Select **Yes** to raise an event if the amount of interval jitter exceeds the threshold that you set. The default is Yes. Interval jitter is the jitter value measured *during* the data collection interval you set. It is not the jitter value at the instance of data collection.
Threshold - Maximum interval jitter	Specify the highest amount of interval jitter that can be achieved before an event is raised. The default is 60 milliseconds.
Event severity when interval jitter exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of interval jitter exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for interval jitter?	Select **Yes** to collect interval jitter data for charts and graphs. When enabled, data collection returns the value of interval jitter measured during the data collection interval. The default is unselected.
Monitor Interval Latency	
Event Notification	
Raise event if interval latency exceeds threshold?	Select **Yes** to raise an event if the amount of interval latency exceeds the threshold that you set. The default is Yes. Interval latency is the latency value measured *during* the data collection interval you set. It is not the latency value at the instance of data collection.
Threshold - Maximum interval latency	Specify the highest amount of interval latency that can be achieved before an event is raised. The default is 400 milliseconds.
Event severity when interval latency exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of interval latency exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for interval latency?	Select **Yes** to collect interval latency data for charts and graphs. When enabled, data collection returns the value of interval latency measured during the data collection interval. The default is unselected.
Monitor Interval Packet Loss	
Event Notification	
Raise event if interval packet loss exceeds threshold?	Select **Yes** to raise an event if the percentage of interval packet loss exceeds the threshold that you set. The default is Yes. Interval packet loss is the percentage of packet loss measured *during* the data collection interval you set. It is not the packet loss value at the instance of data collection.
Threshold - Maximum interval packet loss	Specify the highest percentage of interval packet loss that can occur before an event is raised. The default is 1.0%.

Description	How To Set It
Event severity when interval packet loss exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of interval packet loss exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for interval packet loss?	Select **Yes** to collect interval packet loss data for charts and graphs. When enabled, data collection returns the percentage of interval packet loss measured during the data collection interval. The default is unselected.

RegisteredResources

Use this Knowledge Script to monitor changes in the number of resources registered to a Communication Manager server. Resources include IP stations, remote office stations, attendant consoles, and H.248 media gateways. This script raises an event when a threshold is exceeded. In addition, this script generates datastreams for the following statistics:

- Number of registered IP stations
- Percentage of increase and decrease in number of registered IP stations
- Number of registered IP attendant consoles
- Percentage of increase and decrease in number of registered IP attendant consoles
- Number of registered remote office stations
- Percentage of increase and decrease in number of registered remote office stations
- Number of registered H.248 media gateways
- Percentage of increase and decrease in number of registered H.248 media gateways

Resource Object

AvayaCM Active SPE object

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the RegisteredResources job. The default is 5.
Monitor Registered IP Stations	
Data Collection	
Collect data for registered IP stations?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of IP stations that were registered during the monitoring period. The default is Yes.
Monitor Increase in Registered IP Stations	
Event Notification	
Raise event if increase in registered IP stations exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in registered IP stations exceeds the threshold you set. The default is Yes.
Threshold - Maximum increase in registered IP stations	Specify the highest percentage of increase in registered IP stations that can occur before an event is raised. The default is 10%.

Parameter	How to Set It
Event severity when increase in registered IP stations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in registered IP stations exceeds the threshold. The default is 15.
Data Collection	
Collect data for increase in registered IP stations?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of increase in registered IP stations during the monitoring period. The default is unselected.
Monitor Decrease in Registered IP Stations	
Event Notification	
Raise event if decrease in registered IP stations exceeds threshold?	Select **Yes** to raise an event if the percentage of decrease in registered IP stations exceeds the threshold you set. The default is Yes.
Threshold - Maximum decrease in registered IP stations	Specify the highest percentage of decrease in registered IP stations that can occur before an event is raised. The default is 10%.
Event severity when decrease in registered IP stations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of decrease in registered IP stations exceeds the threshold. The default is 15.
Data Collection	
Collect data for decrease in registered IP stations?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in registered IP stations during the monitoring period. The default is unselected.
Monitor Registered IP Attendant Consoles	
Data Collection	
Collect data for registered IP attendant consoles?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of IP attendant consoles that were registered during the monitoring period. The default is Yes.
Monitor Increase in Registered IP Attendant Consoles	
Event Notification	
Raise event if increase in registered IP attendant consoles exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in registered IP attendant consoles exceeds the threshold you set. The default is Yes.
Threshold - Maximum increase in registered IP attendant consoles	Specify the highest percentage of increase in registered IP attendant consoles that can occur before an event is raised. The default is 10%.
Event severity when increase in registered IP attendant consoles exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in registered IP attendant consoles exceeds the threshold. The default is 15.
Data Collection	
Collect data for increase in registered IP attendant consoles?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of increase in registered IP attendant consoles during the monitoring period. The default is unselected.
Monitor Decrease in Registered IP Attendant Consoles	
Event Notification	

Parameter	How to Set It
Raise event if decrease in registered IP attendant consoles exceeds threshold?	Select **Yes** to raise an event if the percentage of decrease in registered IP attendant consoles exceeds the threshold you set. The default is Yes.
Threshold - Maximum decrease in registered IP attendant consoles	Specify the highest percentage of decrease in registered IP attendant consoles that can occur before an event is raised. The default is 10%.
Event severity when decrease in registered IP attendant consoles exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of decrease in registered IP attendant consoles exceeds the threshold. The default is 15.
Data Collection	
Collect data for decrease in registered IP attendant consoles?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in registered IP attendant consoles during the monitoring period. The default is unselected.
Monitor Registered Remote Office Stations	
Data Collection	
Collect data for registered remote office stations?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of remote office stations that were registered during the monitoring period. The default is Yes.
Monitor Increase in Registered Remote Office Stations	
Event Notification	
Raise event if increase in registered remote office stations exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in registered remote office stations exceeds the threshold you set. The default is Yes.
Threshold - Maximum increase in registered remote office stations	Specify the highest percentage of increase in registered remote office stations that can occur before an event is raised. The default is 10%.
Event severity when increase in registered remote office stations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in registered remote office stations exceeds the threshold. The default is 15.
Data Collection	
Collect data for increase in registered remote office stations?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of increase in registered remote office stations during the monitoring period. The default is unselected.
Monitor Decrease in Registered Remote Office Stations	
Event Notification	
Raise event if decrease in registered remote office stations exceeds threshold?	Select **Yes** to raise an event if the percentage of decrease in registered remote office stations exceeds the threshold you set. The default is Yes.
Threshold - Maximum decrease in registered remote office stations	Specify the highest percentage of decrease in registered remote office stations that can occur before an event is raised. The default is 10%.

Parameter	How to Set It
Event severity when decrease in registered remote office stations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of decrease in registered remote office stations exceeds the threshold. The default is 15.
Data Collection	
Collect data for decrease in registered remote office stations?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in registered remote office stations during the monitoring period. The default is unselected.
Monitor Registered H.248 Media Gateways	
Data Collection	
Collect data for registered H.248 media gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of H.248 media gateways that were registered during the monitoring period. The default is Yes.
Monitor Increase in Registered H.248 Media Gateways	
Event Notification	
Raise event if increase in registered H.248 media gateways exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in registered H.248 media gateways exceeds the threshold you set. The default is Yes.
Threshold - Maximum increase in registered H.248 media gateways	Specify the highest percentage of increase in registered H.248 media gateways that can occur before an event is raised. The default is 10%.
Event severity when increase in registered H.248 media gateways exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in registered H.248 media gateways exceeds the threshold. The default is 15.
Data Collection	
Collect data for increase in registered H.248 media gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of increase in registered H.248 media gateways during the monitoring period. The default is unselected.
Monitor Decrease in Registered H.248 Media Gateways	
Event Notification	
Raise event if decrease in registered H.248 media gateways exceeds threshold?	Select **Yes** to raise an event if the percentage of decrease in registered H.248 media gateways exceeds the threshold you set. The default is Yes.
Threshold - Maximum decrease in registered H.248 media gateways	Specify the highest percentage of decrease in registered H.248 media gateways that can occur before an event is raised. The default is 10%.
Event severity when decrease in registered H.248 media gateways exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of decrease in registered H.248 media gateways exceeds the threshold. The default is 15.
Data Collection	
Collect data for decrease in registered H.248 media gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in registered H.248 media gateways during the monitoring period. The default is unselected.

RemovePhone

Use this Knowledge Script to remove Avaya IP phone objects from the TreeView in the AppManager console. This script raises an event when phones are removed successfully.

Tips

- After running this script on the object you want to remove, double-check your selection in the Objects tab. By specifically selecting a phone object from the Objects tab, you will not accidentally remove a phone that you want to keep.
- Before removing a phone, stop any monitoring jobs that are running on the phone.

Resource Object

AvayaCM Station object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the RemovePhone job. The default is 5.
Event Notification	
Raise event if phones are removed successfully?	Select **Yes** to raise an event if the selected phone objects are successfully removed from the TreeView. The default is Yes.
Event severity when phones are removed successfully	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the selected phone objects are successfully removed from the TreeView. The default is 25.

RetrieveConfigData

Use this Knowledge Script to retrieve configuration data about stations and gateways from the Communication Manager server and store it in the Avaya CM supplemental database.

Prerequisite

Create the supplemental database using the SetupSupplementalDB script or the *Set up supplemental database?* parameters in the Discovery_AvayaCM Knowledge Script.

Resource Object

AvayaCM Active SPE object

Default Schedule

By default, this script runs once a day, at 3 AM, in order to perform CPU-intensive functions when Communication Manager is less busy with call activity or maintenance tasks.

However, because the PhoneDeregistrations script uses the configuration data this script retrieves, this script also runs once, immediately, allowing you to use the PhoneDeregistrations script as soon as possible.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the RetrieveConfigData job. The default is 5.
Enable use of SNMP GETBulk requests?	By default, this parameter is enabled, allowing the RetrieveConfigData Knowledge Script job to use `GETNext` and `GETBulk` SNMP requests to access Communication Manager MIBs. Disable this parameter to allow the script to use only `GETNext` requests. Not all MIB tables are extensive enough to need a `GETBulk` request. A `GETBulk` request is faster, but more CPU-intensive than `GETNext`.
Number of rows to request for each GETBulk operation	Specify the number of rows from the MIB table to return in a `GETBulk` request. The default is 10 rows. The number of rows determines how quickly MIB data is returned. If CPU usage is too high, you can reduce the number of rows per `GETBulk` or disable the *Enable use of SNMP GETBulk requests?* parameter.
Interval to pause between GETBulk operations	Specify the number of milliseconds to wait between GETBulk requests. The default is 100 milliseconds. The amount of delay can help with managing CPU usage and speed of SNMP requests. For example, a one-row `GETBulk` with a 100-millisecond delay between requests executes more slowly and uses less CPU than a `GETNext` request.

Parameter	How to Set It
Raise event if configuration retrieval succeeds?	Select **Yes** to raise an event if the retrieval process succeeds. The default is unselected.
Event severity when configuration retrieval succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which retrieval succeeds. The default is 25.

SecurityViolations

Use this Knowledge Script to monitor the following security violations:

- Barrier code violations
- Calls that generated authorization code violations
- Calls that generated station security code violations

Barrier codes and authorization codes provide a level of security for remote call access to such telephony components as PBXs, switch features, and trunks. Station security codes enable the Personal Station Access feature and the Extended User Administration of Redirected Calls feature.

This script raises an event if a threshold is exceeded. In addition, this script generates datastreams for monitored violations.

Resource Object

AvayaCM Active SPE object

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SecurityViolations job. The default is 5.
Select port type to monitor	Select the type of login port you want to monitor for security violations. Choose from the following: • All (default) • SYSAM-LCL (local port) • SYSAM-RMT (remote port) • MAINT (maintenance port) • SYS-Port (system port) • MGR1 (management terminal connection port) • NET (network controller port) • EPN (EPN maintenance EIA port) • INADS (initialization administration system port)
Enable use of SNMP GETBulk requests?	By default, this parameter is enabled, allowing the SecurityViolations Knowledge Script job to use `GETNext` and `GETBulk` SNMP requests to access Communication Manager MIBs. Disable this parameter to allow the script to use only `GETNext` requests. Not all MIB tables are extensive enough to need a `GETBulk` request. A `GETBulk` request is faster, but more CPU-intensive than `GETNext`.

Parameter	How to Set It
Number of rows to request for each GETBulk operation	Specify the number of rows from the MIB table to return in a `GETBulk` request. The default is 10 rows. The number of rows determines how quickly MIB data is returned. If CPU usage is too high, you can reduce the number of rows per `GETBulk` or disable the *Enable use of SNMP GETBulk requests?* parameter.
Interval to pause between GETBulk operations	Specify the number of milliseconds to wait between GETBulk requests. The default is 100 milliseconds. The amount of delay can help with managing CPU usage and speed of SNMP requests. For example, a one-row `GETBulk` with a 100-millisecond delay between requests executes more slowly and uses less CPU than a `GETNext` request.
Monitor Violations for Barrier Codes	
Event Notification	
Raise event if number of violations for barrier codes exceeds threshold?	Select **Yes** to raise an event if the number of security violations for barrier codes exceeds the threshold you set. The default is Yes.
Threshold - Maximum violations for barrier codes	Specify the highest number of security violations for barrier codes that can occur before an event is raised. The default is 0 violations.
Event severity when number of violations for barrier codes exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of security violations for barrier codes exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of violations for barrier codes?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of security violations for barrier codes that occurred during the monitoring period. The default is unselected.
Monitor Violations for Authorization Codes	
Event Notification	
Raise event if number of calls that generated authorization code violations exceeds threshold?	Select **Yes** to raise an event if the number of calls that generated authorization code violations exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of calls that generated authorization code violations	Specify the highest number of calls that can generate authorization code violations before an event is raised. The default is 0 calls.
Event severity when the number of calls that generated authorization code violations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of calls that generated authorization code violations exceeds the threshold. The default is 15.
Data Collection	
Collect data for the number of calls that generated authorization code violations?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of that generated authorization code violations during the monitoring period. The default is unselected.
Monitor Station Violations	
Event Notification	

Parameter	How to Set It
Raise event if the number of calls that generated station violations exceeds threshold?	Select **Yes** to raise an event if the number of calls that generated station violations exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of calls that generated station violations	Specify the highest number of calls that can generate station violations before an event is raised. The default is 0 calls.
Event severity when the number of calls that generated station violations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of calls that generated station violations exceeds the threshold. The default is 15.
Data Collection	
Collect data for the number of calls that generated station violations?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that generated station violations during the monitoring period. The default is unselected.

SetupSupplementalDB

Use this Knowledge Script to create an Avaya CM supplemental database, including the tables and stored procedures needed to store call detail records (CDRs), disconnected phone information, and deregistered phone information. In addition, this script creates a SQL Server job that removes old records from the supplemental database.

You can also create the Avaya CM supplemental database using the *Set up supplemental database?* parameters in the Discovery_AvayaCM Knowledge Script.

For more information, see "Understanding the Avaya CM Supplemental Database" on page 511.

Resource Object

AvayaCM Active SPE object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SetupSupplementalDB job. The default is 5.
Raise event if database set up succeeds?	Select **Yes** to raise an event if creation of the Avaya CM supplemental database is successful. The default is unselected.
Event severity when database setup succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the success of the creation of the Avaya CM supplemental database. The default is 25.
CDR Parameters	
Number of days to keep call detail records	Specify the number of days' worth of CDRs you want to keep in the Avaya CM supplemental database. Data older than what you specify is discarded. The default is 7 days.
SQL Server Information	

Parameter	How to Set It
Local SQL Server instance name	Specify the name of the local SQL Server instance (on the proxy agent computer) in which you want to create the new Avaya CM supplemental database. Leave this parameter blank to accept the default name.
Start pruning job on supplemental database?	**For all supported versions of SQL Server, except SQL Server 2005 Express**: Set to **Yes** to create a SQL job that deletes data from the supplemental database. The SQL job runs every night. Data is deleted from the supplemental database based on the value you specify in the *Number of days to keep call detail records* parameter. The default is Yes. **For SQL Server 2005 Express**: Set to **No**. The pruning job is not supported for SQL Server 2005 Express. **To manually delete data from the supplemental database**: 1. Run the following stored procedure from a command line: `osql -E -S <sql server> -n -d <database> -Q "exec dbo.Task_AvayaCM_Pruning"` where <*sql server*> is the name of the server that hosts the supplemental database, and where <database> is the name of the supplemental database. For example: `osql -E -S SuppDBAvaya -n -d AvayaCM_S8300-Cluster -Q "exec dbo.Task_AvayaCM_Pruning"` 2. Configure a Windows Scheduled Task to schedule pruning at an interval of your choosing. The process for configuring a Windows Scheduled Task varies according to your version of Microsoft Windows. Consult your Windows documentation for more information.

Understanding the Avaya CM Supplemental Database

The Avaya CM supplemental database is a Microsoft SQL Server database you create on the proxy agent computer. The supplemental database fulfills several functions.

Storage for CDRs and RTCP packets

The managed object on the proxy agent computer receives call detail records (CDRs) from Communication Manager servers and RTCP packets from phones registered to Communication Manager servers. The proxy agent computer saves the CDR and RTCP packet data to tables in the Avaya CM supplemental database. The CallActivity, CallFailures, CallQuality, and CallQuery Knowledge Scripts query the supplemental database for the data they need.

When you start the CallActivity, CallFailures, CallQuality, or CallQuery Knowledge Script job, the managed object begins collecting CDR and RTCP data to store in the Avaya CM supplemental database. After the job stops, the managed object continues to collect CDRs and packet data. Data collection stops within a time period equal to two intervals of the job, but never less than 4 minutes after the job stops.

When you create the supplemental database, you specify how long data is retained before being deleted and archived. AppManager automatically deletes CDRs older than the retention age you specify.

Storage for phone deregistration and disconnection data

The PhoneDeregistrations and PhoneConnectivity Knowledge Scripts use SNMP queries to create lists of phones that are unregistered or registered but disconnected. The scripts query the Avaya CM supplemental database, which is populated by the RetrieveConfigData script with configuration data retrieved from Communication Manager.

To create and use the supplemental database:

1. **Create the database**. Create one Avaya CM supplemental database per Communication Manager cluster you are monitoring. Use the Discovery_AvayaCM or SetupSupplementalDB Knowledge Script for this purpose.
2. **Populate the database**. Use RetrieveConfigData to retrieve configuration data from Communication Manager and save it in the Avaya CM supplemental database.
3. **Monitor the data in the database**. Use the following scripts to analyze the data in the database.
   - CallActivity monitors active and completed calls.
   - CallFailures monitors calls that ended with the condition codes you specify.
   - CallQuality monitors jitter, latency, lost data, and MOS.
   - CallQuery searches for data based on query filters you select.
   - PhoneConnectivity monitors disconnected registered phones and maintains a history of monitored phones in the supplemental database.
   - PhoneDeregistrations monitors phone deregistrations and maintains a history of phone deregistrations in the supplemental database.

SNMPTrap

Use this Knowledge Script to monitor SNMP traps forwarded from NetIQ SNMP Trap Receiver (Trap Receiver). This script raises an event when an SNMP trap is received and when Trap Receiver is unavailable or subsequently becomes available. In addition, this script generates datastreams for Trap Receiver availability.

This script checks for SNMP traps in the MIB tree. You can add Management Information Bases (MIBs) to the MIB tree. For more information, see the AddMIB Knowledge Script.

Trap Receiver receives SNMP traps, filters them, and then forwards the traps to AppManager. For more information, see "Working with NetIQ SNMP Trap Receiver" on page 514.

Resource Object

AvayaCM Trap Receiver object

Default Schedule

By default, this script runs on an asynchronous schedule.

Setting Parameter Values

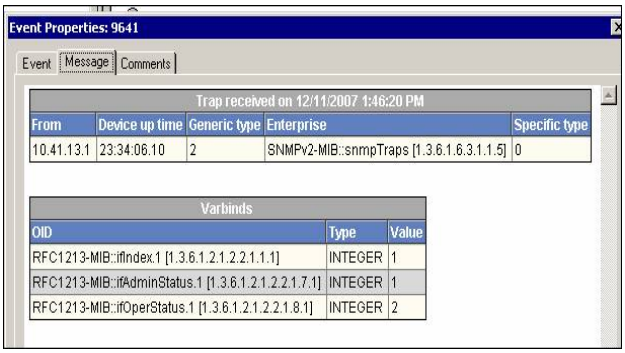
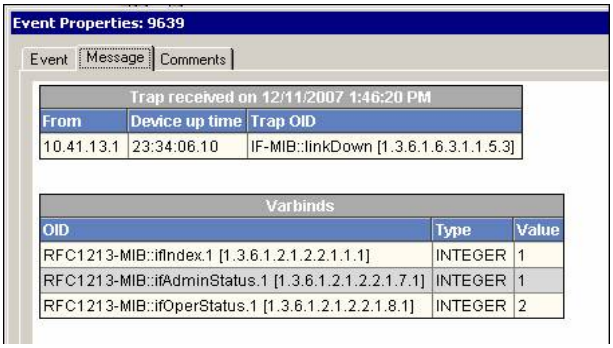
Set the following parameters as needed:

Parameter	How to Set It
Trap Filters	
List of trap OIDs	Use this parameter to provide a list of the OIDs (object identifiers) of the traps you want to monitor. Separate multiple OIDs with a comma. For example: `1.3.6.1.2.1.2.2.1.1.1,1.3.6.1.2.1.2.2.1.7.1`

Full path to file with list of trap OIDs	If you have many OIDs to monitor, use this parameter to identify the full path to a file that contains a list of the OIDs. Each OID in the file should be on a separate line. For example:
	`1.3.6.1.2.1.2.2.1.1.1`
	`1.3.6.1.2.1.2.2.1.7.1`
	Because the file must be accessible from the AppManager agent, the path must be a local directory on the agent computer or a UNC path. The `netiqmc` service must be running as a user that has access to the UNC path.

List of MIB subtrees	Use this parameter to monitor an OID *and* all of its subtrees. Provide a comma-separated list of the OIDs you want to monitor. For example: `1.3.6,1.3.7`

Full path to file with list of MIB subtrees	If you have many subtrees to monitor, use this parameter to provide the full path to a file that contains a list of the OIDs. Each OID in the file should be on a separate line. For example:
	`1.3.6`
	`1.3.7`
	Because the file must be accessible from the AppManager agent, the path must be a local directory on the agent computer or a UNC path. The `netiqmc` service must be running as a user that has access to the UNC path.

Parameter	How to Set It
Event Notification	
Format trap data according to SNMP version	Select the version of SNMP whose formatting should be used for trap event messages. The data provided by each format is the same; only the layout is different. An event message in SNMP v1 format looks like this:  An event message in SNMP v2 format looks like this: 
Include prefix information to format event messages for Netcool adapter?	Select **Yes** to format trap messages for use by IBM Tivoli Netcool. When this option is enabled, trap messages include tokens and separators, such as tildes (~), that Netcool recognizes.
Raise cleared/resolved alarm event?	Select **Yes** to raise an event when the SNMP trap message contains information about a cleared or resolved alarm. The default is Yes.
Event severity when cleared/ resolved alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP trap message contains information about a cleared or resolved alarm. The default is 25.
Raise critical alarm event?	Select **Yes** to raise an event when the SNMP trap message contains information about a critical alarm. The default is Yes.
Event severity when critical alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP trap message contains information about a critical alarm. The default is 5.
Raise major alarm event?	Select **Yes** to raise an event when the SNMP trap message contains information about a major alarm. The default is Yes.
Event severity when major alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP trap message contains information about a major alarm. The default is 10.
Raise minor alarm event?	Select **Yes** to raise an event when the SNMP trap message contains information about a minor alarm. The default is Yes.

Parameter	How to Set It
Event severity when minor alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP trap message contains information about a minor alarm. The default is 15.
Raise warning alarm event?	Select **Yes** to raise an event when the SNMP trap message contains information about a warning alarm. The default is Yes.
Event severity when warning alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP trap message contains information about a warning alarm. The default is 15.
Raise unmapped alarm event?	Select **Yes** to raise an event when an SNMP trap is received but is not reflected in the `.CSV` mapping file. The default is Yes. Disable this parameter if you do not want to be informed about SNMP traps that are not mapped in the `.CSV` file.
Event severity when unmapped alarm received	Set the severity level, from 1 to 40, to indicate the importance of an event in which an SNMP trap is not mapped in the `.CSV` file. The default is 15.
Raise Trap Receiver availability events?	Select **Yes** to raise an event when Trap Receiver becomes unavailable and when Trap Receiver becomes available once again. The default is Yes.
Event severity when Trap Receiver is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes unavailable. The default is 5.
Event severity when Trap Receiver becomes available	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes available after being unavailable. The default is 25.
Data Collection	
Collect data for Trap Receiver availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns “1” if Trap Receiver is available and “0” if Trap Receiver is unavailable. The default is unselected.
Interval for collecting Trap Receiver availability data	Specify the frequency with which the script collects Trap Receiver availability data. The default is every 5 minutes.

Working with NetIQ SNMP Trap Receiver

Installation of AppManager for Avaya Communication Manager automatically installs NetIQ SNMP Trap Receiver (Trap Receiver), which runs as a service: `NetIQTrapReceiver.exe`. Trap Receiver may compete for port usage with any other trap receiver installed on the same computer.

What is NetIQ SNMP Trap Receiver?

In general, a trap receiver is an application that receives traps from SNMP agents. Trap Receiver receives, filters, and forwards SNMP traps to AppManager. When you use Trap Receiver with AppManager for Avaya Communication Manager, the SNMPTrap Knowledge Script raises events when SNMP traps are received.

What is an SNMP Trap?

Simple Network Management Protocol (SNMP) is a protocol-based system used to manage devices on TCP/IP-based networks. From devices on which an SNMP agent resides, such as routers and switches, SNMP sends unsolicited notifications, called traps, to network administrators when thresholds for certain conditions are exceeded. These conditions are defined by the vendor in a device’s Management Information Base (MIB); the network administrator sets the thresholds.

Traps are composed of Protocol Data Units (PDUs). Each PDU contains the following information, organized in various ways depending on the version of SNMP in use:

- SNMP version number
- Community name of the SNMP agent
- PDU type
- Enterprise OID (object identifier), a unique number that identifies an enterprise and its system objects in the MIB
- IP address of the SNMP agent
- Generic trap type: Cold start, Warm start, Link down, Link up, Authentication failure, and Enterprise
- Specific trap type. When the Generic trap type is set to "Enterprise," a specific trap type is included in the PDU. A specific trap is one that is unique or specific to an enterprise.
- Time the event occurred
- Varbind (variable binding), a sequence of two fields that contain the OID and a value

Understanding Trap Receiver Architecture

Trap Receiver operates on a Client-Server architecture: the *Server*—the stand-alone Trap Receiver application—receives, filters, and forwards SNMP traps to the *Client*—an application that receives traps, such as AppManager. The Server may receive traps from standard UDP port 162 or from any other configured port. The Client and the Server can reside on the same computer or on separate (proxy) computers.

Communication between Client and Server is implemented as XML messages over a TCP connection. Only one Server is allowed per computer; however, several Clients are allowed per computer. Clients that are registered to the same Server share the same TCP connection. The Server TCP port should be known to all potential Clients.

Understanding the Trap Receiver Configuration File

The configuration file for Trap Receiver, `NetIQTrapReceiver.conf`, identifies the UDP and TCP ports used by Trap Receiver: the UDP port is used for receiving traps; the TCP port is used for communicating with the Client, such as AppManager or another supported NetIQ application. The configuration file also identifies the level of logging you want to use and whether port forwarding is enabled.

By default, the configuration file is installed in `[`*`installation directory`*`]\config`, and has the following format:

```
#####################################################################
## NetIQTrapReceiver.conf
# A configuration file for NetIQ SNMP Trap Receiver
#####################################################################

#########################
# TCP port
# Syntax: tcp_port [port]
# E.g. : tcp_port 2735
#########################
tcp_port 2735

#########################
# UDP port
# Syntax: udp_port [port]
# E.g. : udp_port 162
#########################
```

```
udp_port 162

#########################
# Forwarding
# Syntax: forward [address]:[port] [v1]
# E.g. : forward 127.0.0.1:1000 v1
#########################

#########################
# Log level
# Syntax: log_level error|warning|info|debug|xml
# E.g. : log_level info
#########################
log_level debug
```

If the configuration file cannot be found, cannot be parsed, or does not contain one of the required values, Trap Receiver is initialized with the default configuration as shown above.

When changing values in the configuration file, take into account the following:

- If you change the TCP port number, stop all asynchronous Knowledge Script jobs associated with the modules that support Trap Receiver. Run the Discovery Knowledge Script on all monitored devices to enable the devices to recognize the new TCP port number.
- If you change the UDP port number, also change the UDP port number configured on the devices that send traps to Trap Receiver.
- If another service uses port 2735 or port 162, Trap Receiver *will not start*. The Trap Receiver log file will contain different levels of messages, based on the log_level you choose. Either change the port numbers in the configuration file, stop the service that is using the default Trap Receiver port numbers, or forward the traps coming in to UDP port 162.
- To forward incoming traps to another trap receiver, such as Microsoft SNMP Trap Service, set the Forwarding values as follows:
  `forward [`*`IP address of other trap receiver`*`]:[`*`port number of other trap receiver`*`] [`*`SNMP version`*`]`.
  For example: `forward 10.40.40.25:167 v1`. By default, incoming traps are not forwarded. For more information, see "Coexisting with Microsoft SNMP Trap Service" on page 516.
- Restart Trap Receiver after any change to the configuration file. From Control Panel, double-click **Administrative Tools** and then double-click **Services**. Right-click **NetIQ Trap Receiver** and select **Restart**.

Coexisting with Microsoft SNMP Trap Service

Two trap receivers cannot be in use on the same computer while using the same standard UDP port (162). If NetIQ SNMP Trap Receiver and another trap receiver such as Microsoft SNMP Trap Service are installed on the same computer and both are receiving traps, then configure Trap Receiver to use the standard UDP port and to forward incoming traps (UDP forwarding) to the other trap receiver. For more information, see "Understanding the Trap Receiver Configuration File" on page 515.

Then, configure the other trap receiver to use a different, non-standard, UDP port that is not in use by another application. The following are instructions for configuring Microsoft SNMP Trap Service.

To configure Microsoft SNMP Trap Service to use another port:

1. Navigate to `c:\Windows\system32\drivers\etc`.
2. Open the **services** file.
3. In the row for `snmptrap`, change the value for **udp** from 162 to another port number that is not in use by any other application. Use the same port number you set as the forwarding port in the Trap Receiver configuration file.

4. Save and close the **services** file.

5. Restart Windows SNMP Trap Service. In Control Panel, double-click **Administrative Tools** and then double-click **Services**. Right-click **SNMP Trap Service** and select **Restart**.

Tip

To see which ports are in use, run `netstat.exe` from a command prompt. Then select an available port as the port for the other trap receiver service.

SystemUptime

Use this Knowledge Script to monitor the number of hours that an Avaya Communication Manager has been operational since its last reboot. This script raises an event if the server reboots. In addition, this script generates a datastream for server uptime.

Resource Object

AvayaCM Server object

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SystemUptime job. The default is 5.
Monitor Reboot Events	
Event Notification	
Raise event if server reboots?	Select **Yes** to raise an event if the Avaya Communication Manager server reboots. The default is Yes.
Event severity when server reboots	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Avaya Communication Manager server reboots. The default is 5.
Monitor Uptime	
Data Collection	
Collect data for uptime?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of time the Avaya Communication Manager server has been operational since its last reboot. The default is Yes.

TrunkGroupUsage

Use this Knowledge Script to monitor the status of a trunk group. This script raises an event if a monitored value exceeds the threshold you set. In addition, this script generates datastreams for the following statistics:

- Total number of hours all trunks are busy with calls
- Percentage of time all trunks are simultaneously in use
- Calls in queue
- Calls not in queue
- Out-of-service trunks

Resource Object

AvayaCM Trunk Group object

Default Schedule

By default, this script runs every hour because the SNMP data it monitors is updated only once an hour. If you change the schedule to a shorter interval, you may receive SNMP request errors until the SNMP data is repopulated.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the TrunkGroupUsage job. The default is 5.
Monitor Total Hours Trunks Busy with Calls	
Event Notification	
Raise event if total hours trunks busy with calls exceeds threshold?	Select **Yes** to raise an event if the total number of hours that all trunks are busy with calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum total hours trunks busy with calls	Specify the highest number of hours that all trunks can be busy with calls before an event is raised. The default is 1 hour.
Event severity when total hours trunks busy with calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the total number of hours that all trunks are busy with calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for total hours trunks busy with calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of hours that all trunks were busy with calls during the monitoring period. The default is Yes.
Monitor Calls Queued	
Event Notification	

Parameter	How to Set It
Raise event if number of calls queued exceeds threshold?	Select **Yes** to raise an event if the number of calls in queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum calls queued	Specify the maximum number of calls that can be in queue before an event is raised. The default is 10 calls.
Event severity when number of calls queued exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of calls in queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for calls queued?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls in queue during the monitoring period. The default is Yes.
Monitor Calls Not Queued	
Event Notification	
Raise event if number of calls not queued exceeds threshold?	Select **Yes** to raise an event if the number of calls not in queue exceeds the threshold you set. The default is Yes. Calls not in queue are calls that were offered to the trunk group when the queue was full.
Threshold - Maximum calls not queued	Specify the maximum number of calls that can be not queued before an event is raised. The default is 5 calls.
Event severity when number of calls not queued exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of calls not queued exceeds the threshold. The default is 15.
Data Collection	
Collect data for calls not queued?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls not queued during the monitoring period. The default is unselected.
Monitor Trunks Out of Service	
Event Notification	
Raise event if number of trunks out of service exceeds threshold?	Select **Yes** to raise an event if the number of out-of-service trunks exceeds the threshold you set. The default is Yes.
Threshold - Maximum trunks out of service	Specify the maximum number of trunks that can be out of service before an event is raised. The default is 1 trunk.
Event severity when number of trunks out of service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of out-of-service trunks exceeds the threshold. The default is 15.
Data Collection	
Collect data for trunks out of service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of trunks that were out of service during the monitoring period. The default is Yes.
Monitor Percent Time Trunks in Use	
Event Notification	
Raise event if percent of time all trunks simultaneously in use exceeds threshold?	Select **Yes** to raise an event if the percentage of time that all trunks are simultaneously in use exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum percent of time all trunks simultaneously in use	Specify the highest percentage of time that all trunks can be simultaneously in use before an event is raised. The default is 1%.
Event severity when percent of time all trunks simultaneously in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of time that all trunks are simultaneously in use exceeds the threshold. The default is 15.
Data Collection	
Collect data for percent of time all trunks simultaneously in use?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of time that all trunks were simultaneously in use during the monitoring period. The default is Yes.

Recommended Knowledge Script Group

The following Knowledge Scripts are members of the AvayaCM recommended Knowledge Script Group (KSG).

- CallActivity
- CPU_Usage
- ESS_Status
- H248GatewayStatus
- LSP_Status
- RegisteredResources
- SecurityViolations
- SystemUptime

The parameters of all scripts in the KSG are set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and run the AvayaCM group on a Communication Manager resource.

Run the KSG on only one cluster at a time. Running the KSG on multiple clusters all at once hinders the proxy agent's ability to spread out processing over time. You can monitor multiple clusters by running the KSG on the first cluster, and then repeating the process for each additional cluster.

The AvayaCM KSG provides a "best practices" usage of AppManager for monitoring your Communication Manager environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView. For more information, see "About Policy-Based Monitoring" in the AppManager Help.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the AvayaCM tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the AvayaCM tab are not affected.

When deployed as part of a KSG, a script's default script parameter settings may differ from when the script is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the AvayaCM KSG and want to restore it to its original form, you can reinstall the AppManager for Avaya Communication Manager module on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\AvayaCM\RECOMMENDED_AvayaCM` directory.

Chapter 13
BackupExec Knowledge Scripts

The BackupExec category provides the following Knowledge Scripts for monitoring Symantec Backup Exec.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AbortedJobs	Monitors the number of aborted or cancelled Backup Exec jobs.
ActiveJobIDs	Monitors the number of jobs that were active when the script ran.
CompletedJobs	Monitors the number of jobs that were completed during the monitoring interval.
FailedJobs	Monitors the number of failed Backup Exec jobs.
IncompleteJobs	Monitors the number of Backup Exec jobs that have not completed.
LatestJob	Scans the Backup Exec log and returns the status of the last completed Backup Exec job.
Report_Availability	Generates a report about Backup Exec availability.
Report_IDsofActiveJobs	Generates a report about the number of active Backup Exec jobs.
Report_NumberofAbortedJobs	Generates a report about the number of aborted Backup Exec jobs.
Report_NumberofCompletedJobs	Generates a report about the number of completed Backup Exec jobs.
Report_NumberofFailedJobs	Generates a report about the number of failed Backup Exec jobs.
Report_NumberofIncompleteJobs	Generates a report about the number of incomplete Backup Exec jobs.
Report_StatusofTheLatestJob	Generates a report about the status of the most-recently-submitted backup job.
ResourceHigh	Monitors the CPU and memory usage of Backup Exec services.
ResubmitFailedJobs	Checks for backup jobs that failed and resubmits those jobs to the Backup Exec server.
ServiceDown	Monitors Backup Exec services to see if they are running.
SkippedFilesInJobs	Monitors the number of files that were skipped during backups that finished within the last monitoring interval.

Knowledge Script	What It Does
SuccessfulJobs	Monitors the number of Backup Exec jobs that completed successfully.
TotalBytes	Monitors the total number of bytes backed up during the last monitoring interval.

About bemcmd.exe

Several Knowledge Scripts need the `bemcmd.exe` applet in order to retrieve information from the Backup Exec sever. This applet ships along with the Symantec Backup Exec software.

With Knowledge Scripts that use `bemcmd.exe,` you cannot configure an interval of less than 5 minutes. This prevents overloading of the Backup Exec server with `bemcmd` requests.

Knowledge Scripts that use `bemcmd.exe` cannot process a completed job history of more than about 350 entries. If they encounter more than about 350 completed job history entries, the following Knowledge Scripts will abort the job:

- CompletedJobs
- SuccessfulJobs
- SkippedFilesInJobs

If a job is aborted due to this limitation, you must delete older job history entries and then try to run the Knowledge Script again.

The following Knowledge Scripts require `bemcmd.exe` in order to run successfully:

- ActiveJobIDs
- CompletedJobs
- ResubmitFailedJobs
- SkippedFilesInJobs
- SuccessfulJobs

AbortedJobs

Use this Knowledge Script to monitor the number of aborted or cancelled Backup Exec jobs and return data about those jobs.

This script periodically scans the Windows Application Event Log for any entries that Backup Exec made regarding aborted or cancelled jobs. When this Knowledge Script starts, it uses the value specified for the **Start with events in past N hours** parameter to determine how to process entries already in the event log. While running at the interval specified on the **Schedule** tab, it scans the event log for any new entries created since the last time it checked.

If the number of cancelled jobs found in the event log exceeds the threshold you set during any monitoring interval, an event is raised.

Resource Object

Backup Exec

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise events. Default is y.
Collect data for number of aborted jobs?	Set to **y** to collect data for reports and graphs. When set to **y**, returns the number of cancelled jobs found. Default is n.
Start with events in past *N* hours	Set this parameter to determine which events are searched the **first** time the Knowledge Script is run. Subsequent searches begin where the last search finished. The following values are valid: • **-1** -- search all Application Event Log events that occur before and during the first monitoring interval. During subsequent monitoring intervals, only events that occur during the interval are searched. • **0** -- search only for events that occur during the monitoring interval; previous events are not searched. • ***N*** -- the number of hours to go back in the event log to scan for matching events. For example, enter 8 to scan the last 8 hours of the event log for matching entries. Default is 0.
Threshold -- Maximum number of aborted jobs	Enter the maximum number of cancelled jobs allowed during any interval before an event is raised. Default is 10 cancelled jobs.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default severity level is 5.

ActiveJobIDs

Use this Knowledge Script to check the number of jobs that are active when the script runs. It does not report all jobs that have been active since this script was last executed.

An "active" job is any job with a status of running, loading, or pending (queued). If the number of active jobs exceeds the maximum threshold or falls below the minimum threshold you set, an event is raised.

This Knowledge Script is useful for verifying that a specific job is still in process. You can also use it to retrieve the job ID of any currently active job.

Note
This script requires bemcmd.exe to run successfully. See "About bemcmd.exe" on page 524for more information.

Resource Object

Backup Exec

Default Schedule

The default interval for this script is **Every 24 hours**. This Knowledge Script must be run at intervals of 5 minutes or more.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold exceeded or not met?	Set to **y** to raise events. Default is y.
Collect data for number of active jobs?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of active jobs, and the job IDs of the active jobs. Default is n.
Threshold -- Maximum number of active jobs	Specify a maximum number of active jobs. If the actual number of active jobs exceeds this threshold, an event is raised. Default is 20 active jobs.
Threshold -- Minimum number of active jobs	Specify a minimum number of active jobs. If the actual number of active jobs falls below this threshold, an event is raised. Default is 5 active jobs.
Event severity when threshold exceeded or not met	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default severity level is 12.

CompletedJobs

Use this Knowledge Script to monitor the number of jobs that were completed during the monitoring interval, regardless of their outcome. A completed job is any job with a status of Cancelled, Successful, or Failed.

If the number of completed jobs exceeds the maximum threshold or falls below the minimum threshold you set, an event is raised.

Note
This script requires bemcmd.exe to run successfully. See "About bemcmd.exe" on page 524for more information.

Resource Object

Backup Exec

Default Schedule

The default interval for this script is **Every 24 hours**. This Knowledge Script must be run at intervals of 5 minutes or more.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold exceeded or not met?	Set to **y** to raise events. Default is y.
Collect data for number of completed jobs?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of completed jobs, and the IDs of the completed jobs. Default is n.
Threshold -- Maximum number of completed jobs	Specify a maximum number of completed jobs. If the number of completed jobs exceeds this threshold, an event is raised. Default is 20 completed jobs.
Threshold -- Minimum number of completed jobs	Specify the minimum number of completed jobs. If the number of completed jobs falls below this threshold, an event is raised. Default is 5 completed jobs.
Event severity when threshold exceeded or not met	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default severity level is 12.

FailedJobs

Use this Knowledge Script to monitor the number of failed Backup Exec jobs and return data about those jobs.

This Knowledge Script periodically scans the Windows Application Event Log for any entries that Backup Exec made regarding failed jobs. When this Knowledge Script starts, it uses the value specified for the **Start with events in past N hours** parameter to determine how to process entries already in the event log. While running at the interval specified on the **Schedule** tab, it scans the event log for any new entries created since the last time it checked.

If the number of failed jobs found in the event log exceeds the threshold you specify during any interval, an event is raised. This Knowledge Script returns the number of failed jobs, and the event detail message shows each job's name, start time, and end time.

Resource Object

Backup Exec

Default Schedule

The default interval for this script is **Every 24 hours.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise events. Default is y.
Collect data for number of failed jobs?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of failed jobs found. Default is n.
Start with events in past *N* hours	Set this parameter to determine which events to search for the **first** time the Knowledge Script is run. Subsequent searches begin where the last search finished. The following values are valid: • **-1** -- search all Application Event Log events that occur before and during the first monitoring interval. During subsequent monitoring intervals, only events that occur during the interval are searched. • **0** -- search only for events that occur during the monitoring interval; previous events are not searched. • ***N*** -- the number of hours to go back in the event log to scan for matching events. For example, enter 8 to scan the last 8 hours of the event log for matching entries. Default is 0.
Threshold -- Maximum number of failed jobs	Specify the maximum number of failed jobs. If the number of failed jobs exceeds this threshold, an event is raised. Default is 10 failed jobs.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default severity level is 5.

IncompleteJobs

Use this Knowledge Script to monitor the number of Backup Exec jobs that have not completed and to return data about those jobs.

This script periodically scans the Backup Exec log for any entries that contain only a data header but no job information. An entry with only a data header indicates that Backup Exec has begun to track the job, but the job is not yet complete.

This Knowledge Script does not determine why the job is not complete. In most cases, however, it indicates that the job is pending (queued) or still running.

If the number of jobs that have not completed exceeds the threshold you set during any interval, an event is raised.

Resource Object

Backup Exec

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise events. Default is y.
Collect data for number of incomplete jobs?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of jobs that have not completed. Default is n.
Threshold -- Maximum number of incomplete jobs	Specify the maximum number of incomplete jobs. If the number of incomplete jobs exceeds this threshold, an event is raised. Default is 2 incomplete jobs.
Event severity when threshold exceeded	If events are enabled, set the event severity level, from 1 to 40, to indicate the importance of the event. Default severity level is 5.

LatestJob

Use this Knowledge Script to monitor the status of the last completed Backup Exec job and return data about that job.

This script periodically scans the Backup Exec log for the status of the last completed backup or restore job. An event is raised if the last job failed. You can set this Knowledge Script to raise an event if the latest job completed successfully.

This Knowledge Script can also monitor the size of the backup file and raise an event if the file exceeds the maximum threshold or falls below the minimum threshold you set. A file that is too large or too small can indicate a problem with the backup.

An event can be raised if the media label on the disk cartridge where the current backup was made is identical to the media label of the disk where the previous backup was made. If the two media labels are identical, it may indicate that the current backup overwrote a previous backup. This Knowledge Script can detect this condition, but only after the first script iteration is complete.

Resource Object

Backup Exec

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if last job ran successfully?	Set this parameter to **y** to raise an event when the last job ran successfully. Default is n. **Note** This script always raises an event when the last job failed.
Collect data for status of last job?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of jobs that have not completed. Default is n.
Threshold -- Maximum size of backup file	Specify the maximum size of the backup file. If the file size exceeds this threshold, an event is raised. Default is 2000 MB.
Threshold -- Minimum size of backup file	Specify the minimum size of the backup file. If the file size falls below this threshold, an event is raised. Default is 10 MB.
Event severity level if...	Set the event severity level, from 1 to 40, to indicate the importance of: • **... last job failed**. Enter a value that indicates the latest job failed. Default is 5. • **... last job succeeded**. Enter a value that indicates the latest job completed successfully. Default is 25. • **... duplicate disk label found**. Enter a value to indicate that the media label of the current backup disk is the same as the media label of the previous backup disk. Default is 15. • **... file size warning**. Enter a value to indicate that the size of the backup file was larger or smaller than the thresholds you set. Default is 18.

Report_Availability

Use this Report Knowledge Script to generate a report about the availability of Backup Exec based on the up and down status of Backup Exec services.

This report uses data collected by the ServiceDown Knowledge Script.

Resource Objects

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Data settings	Use the following parameters to define the statistical calculation applied to data, and which data is displayed.
Hours or percentage on chart	Select whether to illustrate availability by hours or as a percentage.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top *N***: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N*% of data (sorted by default) • **Bottom *N***: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). Default is 25.
Truncate top/bottom?	If set to yes, the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. Default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to yes to include a table in the report that lists parameter settings for the report script. Default is yes.

Description	How to Set It
Include table?	Set to yes to include a table of data stream values in the report. Default is yes.
Include chart?	Set to yes to include a chart of data stream values in the report. The default is yes.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report. Default is pie chart style.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. Adding the job ID to the output folder name is helpful to identify a specific instance of a report Knowledge Script with its corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to yes to append a timestamp to the title of the report, making each title unique. The timestamp consists of the date and time the report was generated. Adding a timestamp lets you run consecutive iterations of the same report without overwriting previous output. Default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to yes to raise an event when the report is successfully generated. Default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_IDsofActiveJobs

Use this Report Knowledge Script to generate a report about the number of active Backup Exec jobs. This report allows you to make a statistical analysis of the data point values (for example, the average or maximum value over a period of time).

This report uses data collected by the BackupExec_ActiveJobIDs Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*.

Default Schedule

The default schedule is **Run once.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computers	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers to be included in your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the aggregation interval (for example, the average value for 1 hour) • **Minimum/Average/Maximum**: Minimum, average, and maximum values of data points for the aggregation interval • **Minimum**: Minimum value of data points for the aggregation interval • **Maximum**: Maximum value of data points for the aggregation interval • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are dispersed from the mean • **Sum**: Total value of data points for the aggregation interval • **Open/Close**: Last value for the aggregation interval • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). Default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. Default is no.
Show totals on the table?	If set to yes, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column Default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. Default is y.
Include table?	Set to **y** to include a table of data stream values in the report. Default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. Default is y.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties as desired.
Add time stamp to title	Set to **y** to append a timestamp to the title of the report. The timestamp consists of the date and time the report was generated. Adding a timestamp lets you run consecutive iterations of the same report without overwriting previous output. Default is n.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **y** to raise an event when the report is successfully generated. Default is y.

Description	How to Set It
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_NumberofAbortedJobs

Use this Report Knowledge Script to generate a report about the number of aborted Backup Exec jobs. This report allows you to make a statistical analysis of the data point values (for example, the average or maximum value over a time period).

This report uses data collected by the BackupExec_AbortedJobs Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*.

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computers	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers to be included in your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the aggregation interval (for example, the average value for 1 hour) • **Minimum/Average/Maximum**: Minimum, average, and maximum values of data points for the aggregation interval • **Minimum**: Minimum value of data points for the aggregation interval • **Maximum**: Maximum value of data points for the aggregation interval • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are dispersed from the mean • **Sum**: Total value of data points for the aggregation interval • **Open/Close**: Last value for the aggregation interval • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). Default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. Default is no.
Show totals on the table?	If set to yes, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column Default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. Default is y.
Include table?	Set to **y** to include a table of data stream values in the report. Default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. Default is y.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties as desired.
Add time stamp to title	Set to **y** to append a timestamp to the title of the report. The timestamp consists of the date and time the report was generated. Adding a timestamp lets you run consecutive iterations of the same report without overwriting previous output. Default is n.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **y** to raise an event when the report is successfully generated. Default is y.

Description	How to Set It
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_NumberofCompletedJobs

Use this Report Knowledge Script to generate a report about the number of completed Backup Exec jobs. This report allows you to make a statistical analysis of the data point values (for example, the average or maximum value over a period of time).

This report uses data collected by the BackupExec_CompletedJobs Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*.

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computers	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the aggregation interval (for example, the average value for 1 hour) • **Minimum/Average/Maximum**: Minimum, average, and maximum values of data points for the aggregation interval • **Minimum**: Minimum value of data points for the aggregation interval • **Maximum**: Maximum value of data points for the aggregation interval • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are dispersed from the mean • **Sum**: Total value of data points for the aggregation interval • **Open/Close**: Last value for the aggregation interval • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). Default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. Default is no.
Show totals on the table?	If set to yes, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column Default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. Default is y.
Include table?	Set to **y** to include a table of data stream values in the report. Default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. Default is y.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties as desired.
Add time stamp to title	Set to **y** to append a timestamp to the title of the report. The timestamp consists of the date and time the report was generated. Adding a timestamp lets you run consecutive iterations of the same report without overwriting previous output. Default is n.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **y** to raise an event when the report is successfully generated. Default is y.

Description	How to Set It
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_NumberofFailedJobs

Use this Report Knowledge Script to generate a report about the number of failed Backup Exec jobs. This report allows you to make a statistical analysis of the data point values (for example, the average or maximum value over a period of time).

This report uses data collected by the BackupExec_FailedJobs Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*.

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computers	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers to be included in your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the aggregation interval (for example, the average value for 1 hour) • **Minimum/Average/Maximum**: Minimum, average, and maximum values of data points for the aggregation interval • **Minimum**: Minimum value of data points for the aggregation interval • **Maximum**: Maximum value of data points for the aggregation interval • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are dispersed from the mean • **Sum**: Total value of data points for the aggregation interval • **Open/Close**: Last value for the aggregation interval • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). Default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. Default is no.
Show totals on the table?	If set to yes, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column Default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. Default is y.
Include table?	Set to **y** to include a table of data stream values in the report. Default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. Default is y.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties as desired.
Add time stamp to title	Set to **y** to append a timestamp to the title of the report. The timestamp consists of the date and time the report was generated. Adding a timestamp lets you run consecutive iterations of the same report without overwriting previous output. Default is n.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **y** to raise an event when the report is successfully generated. Default is y.

Description	How to Set It
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_NumberofIncompleteJobs

Use this Report Knowledge Script to generate a report about the number of incomplete Backup Exec jobs. This report allows you to make a statistical analysis of the data point values (for example, the average or maximum value over a period of time).

This report uses data collected by the BackupExec_IncompleteJobs Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*.

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computers	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers to be included in your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the aggregation interval (for example, the average value for 1 hour) • **Minimum/Average/Maximum**: Minimum, average, and maximum values of data points for the aggregation interval • **Minimum**: Minimum value of data points for the aggregation interval • **Maximum**: Maximum value of data points for the aggregation interval • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are dispersed from the mean • **Sum**: Total value of data points for the aggregation interval • **Open/Close**: Last value for the aggregation interval • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). Default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. Default is no.
Show totals on the table?	If set to yes, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column Default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. Default is y.
Include table?	Set to **y** to include a table of data stream values in the report. Default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. Default is y.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties as desired.
Add time stamp to title	Set to **y** to append a timestamp to the title of the report. The timestamp consists of the date and time the report was generated. Adding a timestamp lets you run consecutive iterations of the same report without overwriting previous output. Default is n.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **y** to raise an event when the report is successfully generated. Default is y.

Description	How to Set It
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_StatusofTheLatestJob

Use this Report Knowledge Script to generate a report about the status of the most recently submitted Backup Exec job. This report lets you make a statistical analysis of the data point values (for example, the average or maximum value over a time period).

This report uses data collected by the AD_LatestJob Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*.

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computers	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers to be included your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the aggregation interval (for example, the average value for 1 hour) • **Minimum/Average/Maximum**: Minimum, average, and maximum values of data points for the aggregation interval • **Minimum**: Minimum value of data points for the aggregation interval • **Maximum**: Maximum value of data points for the aggregation interval • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are dispersed from the mean • **Sum**: Total value of data points for the aggregation interval • **Open/Close**: Last value for the aggregation interval • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). Default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. Default is no.
Show totals on the table?	If set to yes, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column Default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. Default is y.
Include table?	Set to **y** to include a table of data stream values in the report. Default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. Default is y.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphical properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties as desired.
Add time stamp to title	Set to **y** to append a timestamp to the title of the report. The timestamp consists of the date and time the report was generated. Adding a timestamp lets you run consecutive iterations of the same report without overwriting previous output. Default is n.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **y** to raise an event when the report is successfully generated. Default is y.

Description	How to Set It
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

ResourceHigh

Use this Knowledge Script to monitor the CPU and memory usage of the Backup Exec services that were found during discovery. If the CPU or memory utilization associated with a monitored service exceeds one of the thresholds you set, an event is raised.

Resource Object

Backup Exec

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise events. Default is y.
Collect data for CPU and memory utilization?	Set to **y** to collect data for reports and graphs. If set to y, returns the CPU and memory utilization for each monitored service. Default is n.
Threshold -- Maximum CPU utilization	Enter the maximum amount of CPU resources consumed by any single Backup Exec service. If CPU utilization exceeds this threshold, an event is raised. Default is 60%
Threshold -- Maximum memory utilization	Enter the maximum amount of memory consumed by any single Backup Exec service. If memory utilization exceeds this threshold, an event is raised. Default is 6 MB.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default severity level is 8.

ResubmitFailedJobs

Use this Knowledge Script to check for backup jobs that failed. If it finds any failed jobs, this Knowledge Script resubmits those jobs to the Backup Exec server.

Note
To check for--but not resubmit--failed backup jobs, use the FailedJobsKnowledge Script.

With releases of Backup Exec prior to 9.0, resubmitted jobs are restarted with a new job ID. For Backup Exec version 9.0 and later, the same job ID is re-used when the job is re-started.

You can set a threshold for the maximum number of resubmitted jobs during any monitoring interval. If the number of resubmitted jobs exceeds the threshold you set, an event is raised. The Knowledge Script still resubmits all failed jobs, even if an event is raised.

Note
This script requires bemcmd.exe to run successfully. See "About bemcmd.exe" on page 524for more information.

Resource Object

Backup Exec

Default Schedule

The default interval for this script is **Every 24 hours**. This Knowledge Script must be run at intervals of 5 minutes or more.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if jobs resubmitted or if threshold exceeded?	Set to **y** to raise events. Default is y.
Collect data for resubmitted jobs?	Set to **y** to collect data for reports and graphs. If set to y, returns the number of backup jobs that were resubmitted during the monitoring interval. Default is n.
Resubmitted jobs threshold	Specify the maximum number of resubmitted backup jobs. If the number of resubmitted backup jobs exceeds this threshold, an event is raised. Default is 10 resubmitted jobs.
Event severity when any job resubmitted	Set the event severity level, from 1 to 40, to indicate the importance of the event when any failed backup jobs are resubmitted. Default severity level is 12.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the threshold-crossing event. Default severity level is 5.

ServiceDown

Use this Knowledge Script to monitor the availability of Backup Exec services that were found during discovery. You can set this script to automatically restart a service that is not running.

By default, an event is raised if any of the Backup Exec services are down.

Resource Object

Backup Exec

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data for status of services?	Set to **y** to collect data for reports and graphs. If set to y, returns the following values: • **100** (service is up) • **0** (service is down) Default is n.
Restart service if down?	Set to **y** to automatically restart any service that is down. Default is y.
Event severity when...	Set the event severity level, from 1 to 40, to indicate the importance when: • **... attempt to restart fails**. Specify a value that indicates the service is down and AppManager cannot restart it. Default is 5. • **... attempt to restart succeeds**. Specify a value that indicates the service was down and AppManager successfully restarted it. Default is 25. • **... restart parameter is disabled**. Specify a value to indicate the service is down and the "Restart service if down?" parameter is set to n. Default is 18.

SkippedFilesInJobs

Use this Knowledge Script to monitor the number of files that were skipped during backup jobs that finished within the last monitoring interval. You can choose to monitor only successful jobs, only failed jobs, or both. In addition, you can filter by specific job IDs. If the total number of files that were skipped across all monitored jobs exceeds the threshold you set, an event is raised.

- First, this Knowledge Script determines the number of Backup Exec jobs that have completed between the current and last Knowledge Script iteration.
- Then it checks for either successful or failed jobs, depending on how you set the "**Monitor**..." parameters.

  If you enter job IDs for the **Filter by specific job IDs** parameter, this Knowledge Script filters the list of completed jobs it found and only considers the job IDs you specified.
- Finally, it looks for skipped files only within the types of jobs (successful or failed) you selected for monitoring.

If you enter an invalid job ID for the **Filter by specific job IDs** parameter, an error event states which job ID was found to be invalid on the first script iteration; however, the script continues to process the other job IDs that were supplied. Filtering by job ID is only supported on Backup Exec 9.x and later.

You must select **y** for either the **Monitor successful jobs** or the **Monitor failed jobs** parameter.

Note
This script requires bemcmd.exe to run successfully. See "About bemcmd.exe" on page 524for more information.

Resource Object

Backup Exec

Default Schedule

The default interval for this script is **Every 24 hours**. This Knowledge Script must be run at intervals of 5 minutes or more.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise events. Default is y.
Collect data for number of skipped files?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of files skipped during the monitoring interval. Default is n.
Filter: Backup Exec job IDs to include (comma-separated, no spaces)	To monitor only specific jobs, type the job IDs. Separate each job ID with commas, and do not use spaces. For example, enter job IDs in the following format: `{63D3C37C-9524-4D25-ABF8-2E0A42E33A6C}, {43D3B57G-9524-4D25-YGH8-2E0A42E33N6H}` **Note**: This parameter is only supported on Backup Exec 9.x.

Description	How to Set It
Monitor successful jobs?	Enter **y** to monitor only successful jobs. Default is y.
Monitor failed jobs?	Enter **y** to monitor only failed jobs. Default is n.
Threshold -- Maximum number of files skipped	Specify the maximum number of files that can be skipped. If the number of files skipped exceeds this threshold, an event is raised. Default is 10 skipped files.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default severity level is 5.

SuccessfulJobs

Use this Knowledge Script to monitor the number of successful Backup Exec jobs that were completed during the monitoring interval and return data about those jobs. A successful job is any job with a status of `Successful`.

If the number of successful jobs falls below the minimum threshold you set, an event is raised.

Note
This script requires bemcmd.exe to run successfully. See "About bemcmd.exe" on page 524for more information.

Resource Object

Backup Exec

Default Schedule

The default interval for this script is **Every 24 hours**. This Knowledge Script must be run at intervals of 5 minutes or more.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold not met?	Set to **y** to raise events. Default is y.
Collect data for number of successful jobs?	Set to **y** to collect data for reports and graphs. If set to **y**, returns the number of successful jobs, and the IDs of the successful jobs. Default is n.
Threshold -- Minimum number of successful jobs	Specify the minimum number of successful jobs. If the number of successful jobs falls below this threshold, an event is raised. Default is 10 successful jobs.
Event severity when threshold not met	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default severity level is 5.

TotalBytes

Use this Knowledge Script to monitor the total number of bytes of data that were backed up during the last monitoring interval. If the number of bytes exceeds a threshold that you set, an event is raised.

Resource Object

Backup Exec

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise events. Default is y.
Collect data for number of bytes backed up?	Set to **y** to collect data for reports and graphs. If set to y, returns the number of bytes backed up since the last time the script ran. Default is n.
Threshold -- Maximum number of bytes backed up	Specify the maximum number of bytes. If the number of bytes backed up exceeds this threshold, an event is raised. Default is 300 MB.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default severity level is 8.

Chapter 14
BES Knowledge Scripts

Update Definition in User Variables. provides the following Knowledge Scripts: for monitoring BlackBerry Enterprise Server resources. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**:

Knowledge Script	What It Does
BlackberryAgent	Monitors the Blackberry agent log files for hung threads and the server being in STANDBY mode.
DebugLogSearch	Uses regular expressions to search for specified strings in log files.
DebugLogSize	Calculates the total debug log size, and purges log files if they exceed a size or age threshold.
HungThreads	Monitors the BlackBerry Enterprise Server service for hung threads.
InactiveUsers	Monitors the inactive users on a BlackBerry Enterprise Server.
MDSConnections	Monitors usage statistics for device and push connections.
MDSFailures	Monitors failure statistics for MDS connections.
MessageSize	Monitors the average size of messages forwarded and of messages to which replies with text were sent for a user on a BlackBerry Enterprise Server.
OrphanedUsers	Collects information on mismatched users from BlackBerry and Exchange Servers.
Report_EndToEndResponseTime	Generates a report about e-mail round-trip response time.
Report_LastUserCount	Generates a report about the last recorded user count and the percentage of licenses in use for a BlackBerry Enterprise Server.
Report_ServerMessageSummary	Generates a report about message activity on a BlackBerry Enterprise Server, including messages sent, received, filtered, and queued during the monitoring interval.
Report_SRPConnectivity	Generates a report about the percentage of uptime for the connection to the wireless network.
Report_UserMessageSummary	Generates a report about message activity per user on a BlackBerry Enterprise Server, including messages sent, received, filtered, and queued during the monitoring interval.
ResponseTime	Sends a message to a handheld device from the BlackBerry-enabled Exchange mailbox, checks for a reply, and determines end-to-end response time.
ServerActivity	Monitors the number of messages that were forwarded, received, pending, expired, non-deliverable, and filtered by the server, plus the total number of messages processed by the server during a monitoring interval.

Knowledge Script	What It Does
ServiceHealth	Monitors BlackBerry Enterprise Server service health, the amount of memory used, and the percentage of CPU time used by BlackBerry server processes.
SRPConnectionStatus	Monitors the status of the Server Routing Protocol (SRP) connection between the BlackBerry Enterprise Server and the Research in Motion (RIM) wireless infrastructure.
SRPTest	Performs a test of the SRP connection to make sure the wireless network can be reached.
UserActivity	Monitors the number of messages that were forwarded, received, pending, expired, non-deliverable, and filtered per user, plus the total number of messages processed by the server during the monitoring interval.
UserCount	Monitors the number of users on a BlackBerry Enterprise Server and the percentage of licenses used.
UsersWithPendingMessages	Monitors the percentage of users on a BlackBerry Enterprise Server who have messages pending for their handheld devices.

BlackberryAgent

Use this Knowledge Script to monitor a Blackberry agent for hung threads. Hung threads decrease the number of requests that can be concurrently processed by the service. Any thread that starts and then does not finish is considered hung.

This script raises an event only when both the number of hung threads and the wait count (in cycles) exceed the specified thresholds. You also have the option to restart the hung service automatically. If you choose to collect data, this script returns data about the number of hung threads, the thread IDs, and the wait count.

The wait count value that you set in the *Wait count - Cycles to wait before restarting service* parameter refers to the number of cycles that a thread has been blocked. If you enable data collection, this script returns the average wait count for the server. Use this statistic as guidance when you set a wait count.

To find hung threads, this script searches for several event IDs in the Blackberry agent event logs. These IDs are defined in the following table. You can also configure this script to look for additional event IDs. For more information, see "Monitoring Additional Event IDs" on page 573.

Event ID	Explanation
10019 -- All worker threads seem to be blocked	All worker threads are unresponsive and cannot be allocated for work.
10165 -- Thread: main timer thread appears to be blocked	RIM provides little information about this event or what it signifies. The event text mentions a "Queuing alarm" from BlackBerry Messaging.
20266 -- At least one worker thread seems to be blocked (*N*)	One of the worker threads is blocked and unable to process mail. The parameter in parentheses indicates a wait count. The value of this parameter indicates how long the thread has been unresponsive: • 1 = 10 minutes • 2 = 20 minutes • 3 = 30 minutes **Note** The BlackBerry Enterprise Server should automatically free hung threads and resume mail processing unless the Exchange Server is down.
20315 -- Thread: *** No Response *** Thread Id=0xFC, Handle=0x238, WaitCount=7, SCS thread not responding, SCS - duplicate PIN check	An unresponsive worker thread has been found. Until it becomes unblocked, the thread cannot complete its work. The WaitCount indicates how long the thread has been in this state. In situations where the WaitCount value exceeds 10, the thread is unlikely to recover on its own.
30000 -- Hung threads detected	An event with the 30000 ID contains the words "hung threads detected".
30038 -- {0xD3} Thread: *** No Response ***	An unresponsive worker thread has been located. Until it becomes unblocked, the thread cannot complete its work. The condition will most likely be resolved without the need to restart the BlackBerry Enterprise Server.
50020 -- {0xC3} Some worker threads have been blocked for 6 health checks	Worker threads that have been unresponsive for six health checks (60 minutes) have been found.
50023 -- All worker threads of one of the pools seem to be blocked	All the threads assigned to a particular Exchange server are not responding. This could indicate a communication issue with that Exchange server, or it could indicate more widespread issues.

Resource Object

Blackberry agent

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackberryAgent job fails. The default is 5.
Restart BES services if hung threads detected?	Select **Yes** to have this script automatically restart services that have hung threads. Any service that has hung threads that have not become unblocked after the wait count has expired (see the *Wait count* parameter) will then be restarted. The default is unselected. When you enable this parameter, a service may be restarted automatically. However, the blocked thread must also meet one of the following conditions: • One (or both) of the following events is found in the event log: -- 10019: All worker threads seem to be blocked -- 50023: All worker threads of one of the pools seem to be blocked • The wait count you set using the *Wait count -- Cycles to wait before restarting service* parameter has been exceeded by one of the hung threads that was found. • The value you set for the *Hung threads -- Maximum number before restarting service* parameter has been exceeded by the number of hung threads found in the server event log.
Wait count -- Cycles to wait before restarting service	Set a wait count for each hung thread. This script waits the specified number of cycles to detect whether hung threads become unblocked. The default is 3 cycles. **Note** You should plan to run this script for a few days and collect data for average wait count on the server to use as guidance for an appropriate wait count.
Hung threads -- Maximum number before restarting service	Specify the maximum number of hung threads that can be detected for a service before it is automatically restarted. **Notes** • Services are not automatically restarted unless you enable the *Restart service if hung threads detected?* parameter. • You should plan to run this script for a few days and collect data for average hung threads on the server to use as guidance for an appropriate maximum number of hung threads. The default is 5 hung threads.
Raise event if service restart succeeds?	Select **Yes** to raise an event if the attempt to restart services that have hung threads is successful. The default is Yes.
Event severity when service restart succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is restarted successfully. The default is 25.

Parameter	How to Set It
Raise event if service restart fails?	Select **Yes** to raise an event if the attempt to restart services that have hung threads fails. The default is Yes.
Event severity when service restart fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is not restarted. The default is 5.
Raise event if hung thread log entries found?	Select **Yes** to raise an event if event log entries related to hung threads are found. The default is Yes.
Event severity when hung thread log entries found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the log contains entries for hung threads. The default is 15.
Raise event if user name found in hung thread log entries?	Select **Yes** to raise an event if a user name is found in the hung thread log entries. The default is Yes.
Event severity when user name found in hung thread log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a user name is found in the hung thread log entries. The default is 15.
Blackberry High Availability Notification	
Raise event when BlackBerry STANDBY mode detected?	Select **Yes** to raise an event when the BlackBerry Enterprise Server is in STANDBY mode. The default is unselected.
Event severity when BlackBerry STANDBY mode detected	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server is in STANDBY mode. The default is 15.
Raise event when BlackBerry STANDBY mode changed to PRIMARY mode?	Select **Yes** to raise an event when the BlackBerry Enterprise Server mode has changed from STANDBY to PRIMARY. The default is Yes.
Event severity when BlackBerry mode changed to PRIMARY mode.	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server mode has changed to PRIMARY. The default is 15.
Monitor number of hung threads	
Event Notification	
Raise event if number of hung threads exceeds threshold?	Select **Yes** to raise an event if the number of hung threads for any service exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of hung threads	Specify the maximum number of hung threads that can be detected for a service before an event is raised. The default is 5 hung threads.
Event severity when number of hung threads exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of hung threads exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of hung threads?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of hung threads on the server. The default is unselected.
Monitor average thread wait count	
Data Collection	
Collect data for average thread wait count?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average wait count for threads on the server. The default is unselected.

DebugLogSearch

Use this Knowledge Script to search the local debug logs for selected text strings. Restrict the types of debug log entries that raise an event by setting up regular-expression filters. Use the filtering parameters to include or exclude specific text strings. The script help includes examples of common filters. The table below identifies common regular-expression syntax.

Note
The search performed by this script can be highly resource-intensive and is intended for limited use only.

Each time this script runs, it checks the monitored debug log for entries matching your selection criteria and raises an event if matching entries are found. The event detail message returns the text of the log entries found. You can determine the number of entries to return in a single event using the *Number of matches per event* parameter.

This script runs two different ways, depending on the type of schedule you set. When you set an "interval" schedule (such as "Every 24 hours"), the first time this script runs, it sets a starting point for future searches. It does not return any results on the first iteration. As the script continues to run on an interval schedule, only new log entries created since the last interval are checked for matches against the text strings you entered for the filter parameters.

On any other type of schedule, such as "Run once," "Daily," or "Weekly", this script searches all the contents of all the debug log files on the selected Log resource objects. Each resource object often contains many such log files. Such a search may therefore be very resource-intensive.

When data collection is enabled, this script returns the number of log entries found, and the data point detail message returns the text of the log entries.

Using Regular Expression Filters

A regular expression is a pattern that describes a specific portion of text. Create regular-expression filters to limit the types of debug log entries that this Knowledge Script looks for. The filtering parameters let you use regular expressions to include or exclude specific text strings.

You must specify an **Include filter**. Optionally, you can also specify an **Exclude filter**. If you use both filters, the script returns log entries that contain any included search strings *and* do not contain any excluded strings.

The filtering parameters in this script support standard regular-expression syntax. The following table highlights common regular expression types and their usage.

For more information about regular expression syntax, see related Web sites such as www.wikipedia.org/wiki/Regular_expression or www.regular-expressions.info.

Regular Expression Type	Description
Literal	A literal expression consists of a single character that matches the first occurrence of that character in the text string. For example, if the expression is "a" and the text string is "`The gray cat is purring`," then the match is the "a" in "`gray`." All characters are literals except for the following: ".", "|", "*", "?", "+", "(", ")", "{", "}", "[", "]", "^", "$" and "\". These characters are treated as literals when preceded by a "\".
Wildcard	The dot wildcard "." matches any single character except line break characters. For example, the expression "`gr.y`" matches `gray`, `grey`, `gr%y`, and so on.

Regular Expression Type	Description
Repeat	A repeat is an expression that is repeated an arbitrary number of times. • A question mark, “?”, indicates that the preceding character in the expression is optional. For example, the expression “`ba?`” returns “b” or “`ba`”. • An asterisk, “*”, indicates that the preceding character is to be matched zero or more times. For example, the expression “`ba*`” returns all instances of “b”, “`ba`”, “`baaa`”, and so on. • A plus sign, “+”, indicates that the preceding character is to be matched one or more times. The expression “`ba+`” returns all instances of “`ba`” or “`baaaa`”, for example, but not “b”. • Curly braces, {}, indicate a specific amount of repetition. For example, the expression “`a{2}`” returns the letter “a” repeated exactly twice. The expression “`a{2,4}`” returns the letter “a” repeated between 2 and 4 times. The expression “`a{2,}`” returns the letter “a” repeated at least twice, with no upper limit. For example, the expression “`ba{2,4}`” returns “`baa`”, “`baaa`”, and “`baaaa`”.
Non-Greedy Repeat	A non-greedy, or lazy, repeat matches the shortest possible string. Whenever the “extended” regular-expression syntax is in use (which is the default), non-greedy repeats are made possible by appending a “?” after the repeat. For example, the following greedy expression, “`<.+>`”, returns `<EM>test</EM>` from the string `This is a <EM>test</EM>`. To return only the HTML tag, rewrite the expression as a non-greedy repeat, “`<.+?>`” which will match only the `<EM>` in the string.
Parentheses	Use parentheses, or round brackets, to group characters and then apply a repetition operator to the group. For example, the expression “`(ab)*`” returns all of the string “`ababab`”.
Non-Marking Parentheses	Parentheses create sub-expressions, or backreferences, which store part of the string matched by the expression inside the parentheses. To use parentheses to group characters but not create backreferences, use non-marking parentheses: `(?:expression)`. For example, the following expression creates no backreference: `(?:ab)*`
Anchor	Anchors do not match characters. Instead, they match a position before, after, or between characters. They “anchor” the regular expression match at a certain point. • A “^” matches a position before the first character in a text string. For example, the expression “`^a`” applied to the text string `abc` returns “a” because “a” is at the beginning of the text string. The expression “`^b`” applied to the same text string returns no value, because “b” is not at the beginning of the text string. • A “$” matches right after the last character in a text string. For example, the expression “`c$`” applied to the text string abc returns “c” because “c” is at the end of the text string. The expression “`a$`” applied to the same string returns no value, because “a” is not at the end of the text string.

Resource Object

BlackBerry Log

Default Schedule

The default interval is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event when the DebugLogSearch job fails. The default is 5.
Filter name	Specify a name to be used to associate data streams with the filter. If no filter is specified, the job ID is used. The default is none. **Note** Do not specify a filter name that ends in “apostrophe s” (‘s). Filter names that end with “'s” prevent the data details from being shown and cause an error message.

Include filter	Only log entries that contain a text string that matches this regular expression filter are considered for data collection and events.
	By default, no filtering is applied. However, to run this script successfully, you must enter a value for this parameter.
	Examples
	• To find Error event IDs, which are five-digit numbers beginning with “1” (1xxxxx), type the following regular expression:
	`^\[1\d{4}\]*`
	• To find log entries related to hung thread error code 30038, type the following regular expression:
	`^\[30038\].*?Thread:*$`
	Note This field is limited to 10,000 characters.

Exclude filter	Only log entries that do **not** contain a text string that matches this regular expression filter are considered for data collection and events.
	By default, no filtering is applied.
	Examples
	• To find all event IDs **except** for those belonging to Informational events, which are five-digit numbers beginning with “3” (3xxxx), type the following regular expression:
	`^\[3\d{4}\]*`
	• To find all log entries **except** for those related to threads, type the following regular expression:
	`Thread:+`
	Note This field is limited to 10,000 characters.

Number of matches per event	Set the maximum number of debug log entries that can be returned in each event report. For example, if this value is set to 25, and 57 debug log entries are found, three event reports are raised: two reports containing 25 events and one report containing seven events. The default is 50 entries per event message.
Raise event if log matches found?	Select **Yes** to raise an event when log entries that match the filtering criteria are found. The default is Yes.

Parameter	How to Set It
Event severity when log matches found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which log entries that match the filtering criteria are found. The default is 25.
Monitor number of matches	
Event Notification	
Raise event if number of matches exceeds threshold?	Select **Yes** to raise an event when the number of entries in a debug log file exceeds the threshold. The default is Yes.
Threshold -- Maximum number of matches	Specify the maximum number of debug log entries that can match the filtering criteria before an event is raised. Enter a value from 0 to 32000 entries. The default is 10 entries.
Event severity when number of matches exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of debug log entries that match the filtering criteria exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of matches?	Select **Yes** to collect data for charts and reports. If enabled, data collection, returns the number of matching debug log entries. The data details include the text of the entries. The default is unselected.

DebugLogSize

Use this Knowledge Script to monitor the size, in MB, of BlackBerry debug logs.

If data collection is enabled, a different data stream is created for each log file. The total size on disk of all monitored logs is also returned. An event is raised if the size threshold you set is exceeded.

This script can automatically purge log files when a log exceeds both a size and age threshold you set. An event is raised if an automatic purge is performed.

Resource Object

BlackBerry Log

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event when the DebugLogSize job fails. The default is 5.
Automatically purge log files?	Select **Yes** to automatically purge a log file if its size exceeds the *Log file size* and if its age exceeds the *Log file age* you set. The default is unselected.
Log file size -- Maximum size before purging	Specify the largest size that the log file can attain before it is purged. **Note** The *Log file age* value must also be met before the purge is performed. The default is 100 MB.
Log file age -- Maximum age before purging	Specify the maximum age that the log file can attain before it is purged. **Note** The *Log file size* value must also be met before the purge is performed. The default is 180 days.
Raise event if log files purged?	Select **Yes** to raise an event if a log file exceeds the size and age limits you set and is subsequently purged. The default is Yes.
Event severity when log files purged	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a log file is purged. The default is 25.
Monitor size of log file	
Event Notification	
Raise event if size of log file exceeds threshold?	Select **Yes** to raise an event if the log file size exceeds the threshold you set.
Threshold -- Maximum size of log file	Specify the maximum size, in Megabytes, that the monitored log file can reach before an event is raised. The default is 100 MB.

Parameter	How to Set It
Event severity when size of log file exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the size of the log file exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for size of log file?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the size of the log file. The default is unselected.
Monitor total size of all monitored log files	
Event Notification	
Raise event if size of all monitored log files exceeds threshold?	Select **Yes** to raise an event if the log file size exceeds the threshold you set. The default is Yes.
Threshold -- Maximum total size of all monitored log files	Specify the maximum size, in Megabytes, that the total of all monitored log files can reach before an event is raised. The default is 1000 MB.
Event severity when total size of all monitored log files exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the combined size of all log files exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for total size of all monitored log files?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total size of all the log files selected for monitoring. The default is unselected.
Monitor number of log files purged	
Event Notification	
Raise event if number of log files purged exceeds threshold?	Select **Yes** to raise an event if the number of log files automatically purged exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of log files purged	Specify the maximum number of log files that can be purged because they have exceeded the size and age thresholds before an event is raised. The default is 10 log files purged.
Event severity when number of log files purged exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of purged log files exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of log files purged?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of log files that were automatically purged when they exceeded the size and age thresholds you set. The data details contain the file names of logs that were removed. The default is unselected.

HungThreads

Use this Knowledge Script to monitor the BlackBerry Enterprise Server service for hung threads. Hung threads decrease the number of requests that can be concurrently processed by the service. Any thread that starts and then does not finish is considered hung.

This script raises an event when hung threads are detected and when the number of hung threads exceeds the threshold you set. You also have the option to restart the hung service automatically. If you choose to collect data, this script returns data about the number of hung threads, the thread ID, and the wait count.

Notes

- This script does not search for hung threads associated with MDS, Collaboration, MailStore, and Administration services.
- This script monitors BlackBerry Attachment and BlackBerry Router services for hung threads if the BlackBerry Enterprise Server is running in STANDBY mode.

The wait count value that you set in the *Wait count - Cycles to wait before restarting service* parameter refers to the number of cycles that a thread has been blocked. If you enable data collection, this script returns the average wait count for the server. Use this statistic as guidance when you set a wait count.

To find hung threads, this script searches for the following event IDs in the BlackBerry Enterprise Server event logs. These IDs are defined in the following table. You can also configure this script to look for additional event IDs. For more information, see "Monitoring Additional Event IDs" on page 573.

Event ID	Explanation
10019 -- All worker threads seem to be blocked	All worker threads are unresponsive and cannot be allocated for work.
10165 -- Thread: main timer thread appears to be blocked	RIM provides little information about this event or what it signifies. The event text mentions a "Queuing alarm" from BlackBerry Messaging.
20266 -- At least one worker thread seems to be blocked (*N*)	One of the worker threads is blocked and unable to process mail. The parameter in parentheses indicates a wait count. The value of this parameter indicates how long the thread has been unresponsive: • 1 = 10 minutes • 2 = 20 minutes • 3 = 30 minutes **Note** The BlackBerry Enterprise Server should automatically free hung threads and resume mail processing unless the Exchange Server is down.
20315 -- Thread: *** No Response *** Thread Id=0xFC, Handle=0x238, WaitCount=7, SCS thread not responding, SCS - duplicate PIN check	An unresponsive worker thread has been found. Until it becomes unblocked, the thread cannot complete its work. The WaitCount indicates how long the thread has been in this state. In situations where the WaitCount value exceeds 10, the thread is unlikely to recover on its own.
30000 -- Hung threads detected	An event with the 30000 ID contains the words "hung threads detected".
30038 -- {0xD3} Thread: *** No Response ***	An unresponsive worker thread has been located. Until it becomes unblocked, the thread cannot complete its work. The condition will most likely be resolved without the need to restart the BlackBerry Enterprise Server.

Event ID	Explanation
50020 -- {0xC3} Some worker threads have been blocked for 6 health checks	Worker threads that have been unresponsive for six health checks (60 minutes) have been found.
50023 -- All worker threads of one of the pools seem to be blocked	All the threads assigned to a particular Exchange server are not responding. This could indicate a communication issue with that Exchange server, or it could indicate more widespread issues.

Resource Object

BlackBerry Enterprise Server service

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event when the HungThreads job fails. The default is 5.
Restart service if hung threads detected?	Select **Yes** to have this script automatically restart services that have hung threads. Any service that has hung threads that have not become unblocked after the wait count has expired (see the *Wait count* parameter) will then be restarted. The default is unselected. When you enable this parameter, a service may be restarted automatically; however, the blocked thread must also meet one of the following conditions: • One (or both) of the following events is found in the event log: -- 10019: All worker threads seem to be blocked -- 50023: All worker threads of one of the pools seem to be blocked • The wait count you set using the *Wait count -- Cycles to wait before restarting service* parameter has been exceeded by one of the hung threads that was found. • The value you set for the *Hung threads -- Maximum number before restarting service* parameter has been exceeded by the number of hung threads found in the server event log.
Wait count -- Cycles to wait before restarting service	Set a wait count for each hung thread. This script waits the specified number of cycles to detect whether hung threads become unblocked. The default is 3 cycles. **Note** You should run this script for a few days and collect data for average wait count on the server to use as guidance for an appropriate wait count.

Parameter	How to Set It
Hung threads -- Maximum number before restarting service	Specify the maximum number of hung threads that can be detected for a service before it is automatically restarted. **Notes** • Services are not automatically restarted unless you enable the *Restart service if hung threads detected?* parameter. • You should plan to run this script for a few days and collect data for average hung threads on the server to use as guidance for an appropriate maximum number of hung threads. The default is 5 hung threads.
Raise event if service restart succeeds?	Select **Yes** to raise an event if the attempt to restart services that have hung threads is successful. The default is Yes.
Event severity when service restart succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which services are restarted successfully. The default is 25.
Raise event if service restart fails?	Select **Yes** to raise an event if the attempt to restart services that have hung threads fails. The default is Yes.
Event severity when service restart fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which services cannot be restarted. The default is 5.
Raise event if hung thread log entries found?	Select **Yes** to raise an event if event log entries related to hung threads are found. The default is Yes.
Event severity when hung thread log entries found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the log contains entries for hung threads. The default is 15.
Raise event if user name found in hung thread log entries?	Select **Yes** to raise an event if a user name is found in the hung thread log entries. The default is Yes.
Event severity when user name found in hung thread log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a user name is found in the hung thread log entries. The default is 15.
Blackberry High Availability Notification	
Raise event when BlackBerry STANDBY mode detected?	Select **Yes** to raise an event when the BlackBerry Enterprise Server is in STANDBY mode. The default is unselected.
Event severity when BlackBerry STANDBY mode detected	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server is in STANDBY mode. The default is 15.
Raise event when BlackBerry STANDBY mode changed to PRIMARY mode?	Select **Yes** to raise an event when the BlackBerry Enterprise Server mode has changed from STANDBY to PRIMARY. The default is Yes.
Event severity when BlackBerry mode changed to PRIMARY mode.	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server mode has changed to PRIMARY. The default is 15.
Monitor number of hung threads	
Event Notification	
Raise event if number of hung threads exceeds threshold?	Select **Yes** to raise an event if the number of hung threads for any service exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of hung threads	Specify the maximum number of hung threads that can be detected for a service before an event is raised. The default is 5 hung threads.
Event severity when number of hung threads exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of hung threads exceeds the threshold you set. The default is 5.
Data Collection	

Parameter	How to Set It
Collect data for number of hung threads?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of hung threads on the server. The default is unselected.
Monitor average thread wait count	
Data Collection	
Collect data for average thread wait count?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average wait count for threads on the server. The default is unselected.

Monitoring Additional Event IDs

By default, the BlackberryAgent and HungThreads Knowledge Scripts look for the following event IDs in the events logs for the BlackBerry agent and the BlackBerry Enterprise Server service:

- 10019
- 10165
- 20266
- 20315
- 30000
- 30038
- 50020
- 50023

You can customize these scripts to look for additional event IDs by altering the `beserrorcodes.xml` file, which is installed by default in `ProgramFiles\AppManager\NetIQ\bin`. In the XML file, you can indicate which event ID to look for and assign an event action to an event ID.

The `beserrorcodes.xml` file has the following format:

```
<?xml version="1.0" encoding="utf-8" ?>
<BES>
    <HungThreads>
      <!-- The Event tag value should be a Perl regular expression for search criteria.-->
      <!-- Action="Restart" will trigger service to be restarted-->
      <Event Action="Restart">^\[10019\].*?All worker threads seem to be blocked.*$</Event>
      <Event>^\[10165\].*?Thread: main timer thread appears to be blocked.*$ </Event>
      <Event>^\[20266\].*?At least one worker thread seems to be blocked.*$</Event>
      <Event>^\[20315\].*?Thread: \*\*\* No Response \*\*\* Thread Id=.*?, Handle=.*?, WaitCount=\d+.*$
</Event>
      <Event>^\[30038\].*?Thread: \*\*\* No Response \*\*\*.*$</Event>
      <Event>^\[50020\].*?Some worker threads have been blocked for \d+ health checks.*$ </Event>
      <Event Action="Restart">^\[50023\].*?All worker threads of one of the pools seem to be blocked.*$
</Event>
      <Event>^\[30000\].*?hung threads detected.*$</Event>
    </HungThreads>
</BES>
```

- where `<BES>` is the document name and a mandatory section.
- where `<HungThreads>` is a mandatory section for the HungThreads and BlackberryAgent Knowledge Scripts.
- where `<Event>` identifies the search criteria.

- where `<Event Action="Restart">` indicates that a service will be restarted if a service's log file contains at least one entry of this event in its log file.

To monitor additional event IDs:

1. Navigate to `ProgramFiles\AppManager\NetIQ\bin` and open `beserrorcodes.xml` in an XML editor.
2. Add a new row using the format shown in the graphic above. Use a Perl regular expression to indicate the event ID you want to monitor, and assign an event action if necessary.
3. Save and close the file. Do not save it with a new name.

InactiveUsers

Use this Knowledge Script to determine which BlackBerry users have been inactive for a specified period of time.

Inactivity is determined by the times of the last message forwarded or of the last device interaction. You can set thresholds for each inactivity measurement. If you enable data collection, this script returns the following data streams for each user:

- The number of days since the last device interaction
- The number of days since the last message forwarded to this user

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event when the InactiveUsers job fails. The default is 5.
Blackberry High Availability Notification	
Raise event when BlackBerry STANDBY mode detected?	Select **Yes** to raise an event when the BlackBerry Enterprise Server is in STANDBY mode. The default is unselected.
Event severity when BlackBerry STANDBY mode detected	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server is in STANDBY mode. The default is 15.
Raise event when BlackBerry STANDBY mode changed to PRIMARY mode?	Select **Yes** to raise an event when the BlackBerry Enterprise Server mode has changed from STANDBY to PRIMARY. The default is Yes.
Event severity when BlackBerry mode changed to PRIMARY mode.	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server mode has changed to PRIMARY. The default is 15.
Database login	If you want to use SQL authentication, supply login information to access the BlackBerry Enterprise Server database. **Note** This information must already be configured in AppManager Security Manager.

Parameter	How to Set It
Mirror database login	To use SQL authentication in a mirrored database environment, supply login information to access the BlackBerry Enterprise Server secondary database. If left blank, Windows authentication is used. **Note** This information must already be configured in AppManager Security Manager.
Maximum number of users to record data streams for	Specify the maximum number of users to include when collecting data. When data collection is enabled, this script returns the time of the last message forwarded to each user on the server. This parameter sets an upper limit on the number of users for whom such data should be collected and returned. The default is 100 users.
Monitor time since last message forwarded	
Event Notification	
Raise event if time since last message forwarded exceeds threshold?	Select **Yes** to raise an event if the time since a user account last forwarded a message exceeds the threshold you set. The default is Yes.
Threshold -- Maximum time since last message forwarded	Specify the maximum number of days that a user can be inactive (defined as the last time that user's account has forwarded a message) before an event is raised. The default is 30 days.
Event severity when time since last message forwarded exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of days that a user has been inactive exceeds the threshold. The default is 5.
Data Collection	
Collect data for time since last message forwarded?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the time that the last message was forwarded to each user. The default is unselected.
Monitor time since last device interaction?	
Event Notification	
Raise event if time since last device interaction exceeds threshold?	Select **Yes** to raise an event if the time since a user last interacted with a BlackBerry device exceeds the threshold you set. The default is Yes.
Threshold -- Maximum time since last device interaction	Specify the maximum number of days that a user can be inactive (defined as the last time a device interaction was associated with that user) before an event is raised. The default is 30 days.
Event severity when time since last device interaction exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of days a user is inactive exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for time since last device interaction?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the time of the last device interaction for each user. The default is unselected.

MDSConnections

Use this Knowledge Script to monitor the BlackBerry Mobile Data Service (MDS) for the number of device and push connections, as well as the maximum packet size and the number of packets for these connections.

Although they both monitor the Mobile Data Service, this script is independent of the MDSFailures Knowledge Script. Therefore, failures may be occurring even if this script shows that connections are succeeding.

MDS usage statistics are stored by the BlackBerry configuration database every 15 minutes. Therefore, this script cannot operate at intervals of less than 15 minutes. Furthermore, this script collects data only for fully completed intervals. For example, if the script is scheduled to run at 1:35 on a 15-minute interval, only the last completed 15-minute interval is recorded, for the period of 1:15 to 1:30.

If data is collected, this script returns the number of connections, the total packet size in bytes, and the number of packets from connections.

Even if you enable data collection, this script may not collect any data. At times, this script returns "null" data, which indicates that the database query returned no rows.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MDSConnections job fails. The default is 5.
Blackberry High Availability Notification	
Raise event when BlackBerry STANDBY mode detected?	Select **Yes** to raise an event when the BlackBerry Enterprise Server is in STANDBY mode. The default is unselected.
Event severity when BlackBerry STANDBY mode detected	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server is in STANDBY mode. The default is 15.
Raise event when BlackBerry STANDBY mode changed to PRIMARY mode?	Select **Yes** to raise an event when the BlackBerry Enterprise Server mode has changed from STANDBY to PRIMARY. The default is Yes.
Event severity when BlackBerry mode changed to PRIMARY mode.	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server mode has changed to PRIMARY. The default is 15.

Parameter	How to Set It
Database login	To use SQL authentication, supply login information to access the BlackBerry Enterprise Server database. **Note** This information must already be configured in AppManager Security Manager.
Mirror database login	To use SQL authentication in a mirrored database environment, supply login information to access the BlackBerry Enterprise Server secondary database. If left blank, Windows authentication is used. **Note** This information must already be configured in AppManager Security Manager.
Monitor number of device connections?	
Event Notification	
Raise event if number of device connections exceeds threshold?	Select **Yes** to raise an event if the number of device connections to the MDS exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of device connections	Specify the maximum number of device connections that can be running to the MDS before an event is raised. The default is 50 connections.
Event severity when number of device connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of device connections exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of device connections?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of device connections to the MDS. The default is unselected.
Monitor number of push connections?	
Event Notification	
Raise event if number of push connections exceeds threshold?	Select **Yes** to raise an event if the number of push connections to the MDS exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of push connections	Specify the maximum number of push connections that can be running to the MDS before an event is raised. The default is 50 connections.
Event severity when number of push connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of push connections exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of push connections?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of push connections to the MDS. The default is unselected.
Monitor packet size for device connections?	
Event Notification	
Raise event if packet size for device connections exceeds threshold?	Select **Yes** to raise an event if the maximum packet size for device connections to the MDS exceeds the threshold you set. The default is Yes.
Threshold -- Maximum packet size for device connections	Specify the maximum size, in Kilobytes, of a packet sent in a device connection to the MDS before an event is raised. The default is 2048 KB.
Event severity when packet size for device connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which packet size exceeds the threshold. The default is 5.

Parameter	How to Set It
Data Collection	
Collect data for packet size for device connections?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total packet size for device connections and the number of packets from device connections. The default is unselected.
Monitor packet size for push connections?	
Event Notification	
Raise event if packet size for push connections exceeds threshold?	Select **Yes** to raise an event if the maximum packet size for push connections to the MDS exceeds the threshold you set. The default is Yes.
Threshold -- Maximum packet size for push connections	Specify the maximum size, in Kilobytes, of a packet sent in a push connection to the MDS before an event is raised. The default is 2048 KB.
Event severity when packet size for push connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which packet size exceeds the threshold. The default is 5.
Data Collection	
Collect data for packet size for push connections?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total packet size for push connections and the number of packets from push connections. The default is unselected.
Monitor number of packets from device connections?	
Event Notification	
Raise event if number of packets from device connections exceeds threshold?	Select **Yes** to raise an event if the number of packets from device connections to the MDS exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of packets from device connections	Specify the maximum number of packets from device connections to the MDS before an event is raised. The default is 1024 packets.
Event severity when number of packets from device connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of packets exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of packets from device connections?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of packets from device connections. The default is unselected.
Monitor number of packets from push connections?	
Event Notification	
Raise event if number of packets from push connections exceeds threshold?	Select **Yes** to raise an event if the number of packets from push connections to the MDS exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of packets from push connections	Specify the maximum number of packets from push connections to the MDS before an event is raised. The default is 1024 packets.
Event severity when number of packets from push connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of packets exceeds the threshold. The default is 5.

Parameter	How to Set It
Data Collection	
Collect data for number of packets from push connections?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of packets from push connections. The default is unselected.

MDSFailures

Use this Knowledge Script to monitor the BlackBerry Mobile Data Service (MDS) for connection failures, device authentication failures, and bad packets sent to handheld devices.

Although they both monitor the Mobile Data Service, this script is completely independent of the MDSConnections Knowledge Script. Therefore, this script may indicate that failures are occurring even if the MDSConnections Knowledge Script shows that connections are succeeding.

MDS usage statistics are stored by the BlackBerry config database every 15 minutes. Therefore, this script cannot operate at intervals of less than 15 minutes. Furthermore, this script collects data only for fully completed intervals. For example, if the script is scheduled to run at 1:35 on a 15-minute interval, only the last completed 15-minute interval is recorded, for the period of 1:15 to 1:30.

If data is collected, this script returns the number of failed and truncated connections, the number of authentication failures, and the number of refused and invalid packets.

Even if you enable data collection, this script may not collect any data. At times, this script returns "null" data, which indicates that the database query returned no rows.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MDSFailures job fails. The default is 5.
Blackberry High Availability Notification	
Raise event when BlackBerry STANDBY mode detected?	Select **Yes** to raise an event when the BlackBerry Enterprise Server is in STANDBY mode. The default is unselected.
Event severity when BlackBerry STANDBY mode detected	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server is in STANDBY mode. The default is 15.
Raise event when BlackBerry STANDBY mode changed to PRIMARY mode?	Select **Yes** to raise an event when the BlackBerry Enterprise Server mode has changed from STANDBY to PRIMARY. The default is Yes.
Event severity when BlackBerry mode changed to PRIMARY mode.	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server mode has changed to PRIMARY. The default is 15.

Parameter	How to Set It
Database login	To use SQL authentication, supply login information to access the BlackBerry Enterprise Server database. If left blank, Windows authentication is used. **Note** This information must already be configured in AppManager Security Manager.
Mirror database login	To use SQL authentication in a mirrored database environment, supply login information to access the BlackBerry Enterprise Server secondary database. If left blank, Windows authentication is used. **Note** This information must already be configured in AppManager Security Manager.
Monitor number of failed connections	
Event Notification	
Raise event if number of failed connections exceeds threshold?	Select **Yes** to raise an event if the number of failed connections to the MDS exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of failed connections	Specify the maximum number of connections to the MDS that can fail before an event is raised. The default is 25 connections.
Event severity when number of failed connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of failed connections exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of failed connections?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of failed connections to the MDS. The default is unselected.
Monitor number of truncated connections	
Event Notification	
Raise event if number of truncated connections exceeds threshold?	Select **Yes** to raise an event if the number of truncated connections to the MDS exceeds the threshold you set. The default is Yes. A truncated connection is one that starts but stops unexpectedly.
Threshold -- Maximum number of truncated connections	Specify the maximum number of connections to the MDS that can be truncated before an event is raised. The default is 25 connections.
Event severity when number of truncated connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of truncated connections exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of truncated connections?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of truncated connections to the MDS. The default is unselected.
Monitor number of authentication failures	
Event Notification	
Raise event if number of authentication failures exceeds threshold?	Select **Yes** to raise an event if the number of authentication failures at the MDS exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of authentication failures	Specify the maximum number of authentication failures that can occur at the MDS before an event is raised. The default is 10 failures.
Event severity when number of authentication failures exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of authentications failures exceeds the threshold you set. The default is 5.

Parameter	How to Set It
Data Collection	
Collect data for number of authentication failures?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of authentication failures at the MDS. The default is unselected.
Monitor number of refused packets	
Event Notification	
Raise event if number of refused packets exceeds threshold?	Select **Yes** to raise an event if the number of packets refused by the MDS exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of refused packets	Specify the maximum number of packets that can have been refused by the MDS before an event is raised. The default is 1024 packets.
Event severity when number of refused packets exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of refused packets exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of refused packets?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of packets refused by the MDS. The default is unselected.
Monitor number of invalid packets	
Event Notification	
Raise event if number of invalid packets exceeds threshold?	Select **Yes** to raise an event if the number of invalid packets received by the MDS exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of invalid packets	Specify the maximum number of invalid packets that can be received by the MDS before an event is raised. The default is 1024 packets.
Event severity when number of invalid packets exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of invalid packets exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of invalid packets?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of invalid packets received by the MDS. The default is unselected.

MessageSize

Use this Knowledge Script to find the average size, in KB, of the messages forwarded and those that were replied to with text per user on a BlackBerry server. This script raises an event if the average message size exceeds the threshold you set.

Resource Object

BlackBerry server

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MessageSize job fails. The default is 40.
Maximum number of users to record data streams for	Specify the maximum number of users on the selected BlackBerry server for whom this Knowledge Script should create data streams. The default is 100.
Blackberry High Availability Notification	
Raise event when BlackBerry STANDBY mode detected?	Select **Yes** to raise an event when the BlackBerry Enterprise Server is in STANDBY mode. The default is unselected.
Event severity when BlackBerry STANDBY mode detected	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server is in STANDBY mode. The default is 15.
Raise event when BlackBerry STANDBY mode changed to PRIMARY mode?	Select **Yes** to raise an event when the BlackBerry Enterprise Server mode has changed from STANDBY to PRIMARY. The default is Yes.
Event severity when BlackBerry mode changed to PRIMARY mode.	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server mode has changed to PRIMARY. The default is 15.
Monitor size of forwarded messages for a user	
Event Notification	
Raise event if average size of forwarded messages exceeds threshold?	Select **Yes** to raise an event if the average size of messages forwarded to a user on the BlackBerry server exceeds the threshold you set. The default is Yes.
Threshold -- Maximum average size of forwarded messages	Specify the maximum average size that messages forwarded to a user on the BlackBerry server can reach before an event is raised. The default is 1024 KB.
Event severity when average size of forwarded messages exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average size of forwarded messages exceeds the threshold you set. The default is 5.
Data Collection	

Parameter	How To Set It
Collect data for average size of forwarded messages for a user?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average size, in KB, of messages forwarded per user on the BlackBerry server. The default is unselected.
Monitor size of messages replied to with text for a user	
Event Notification	
Raise event if average size of messages replied to with text exceeds threshold?	Select **Yes** to raise an event if the average size of messages to which replies with text were sent by a user on the BlackBerry server exceeds the threshold you set. The default is unselected.
Threshold -- Maximum average size of messages replied to with text	Specify the maximum average size that messages to which replies with text were sent can reach for a user on the BlackBerry server before an event is raised. The default is 25 connections.
Event severity when average size of messages replied to with text exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average size of messages exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for average size of messages replied to with text for a user?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average size, in KB, of messages to which replies with text were sent by a user on the BlackBerry server. The default is unselected.

OrphanedUsers

Use this script to determine which BlackBerry users have been orphaned. "Orphaned" users are those whose BlackBerry accounts no longer have matching, valid Exchange accounts.

If data collection is enabled, this script returns the number of BlackBerry users that have been orphaned. Further information about each orphaned user is returned in the data details for the data stream.

You must have a valid MAPI profile set up on the server where you are running the job. This profile is part of the requirements for installing the BlackBerry server. Consult your BlackBerry Enterprise Server documentation for instructions about obtaining the name of this profile, which you need to enter for the *MAPI profile* parameter.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the OrphanedUsers job fails. The default is 5.
MAPI profile	Enter the name of the MAPI profile you are using on the BlackBerry server.
Blackberry High Availability Notification	
Raise event when BlackBerry STANDBY mode detected?	Select **Yes** to raise an event when the BlackBerry Enterprise Server is in STANDBY mode. The default is unselected.
Event severity when BlackBerry STANDBY mode detected	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server is in STANDBY mode. The default is 15.
Raise event when BlackBerry STANDBY mode changed to PRIMARY mode?	Select **Yes** to raise an event when the BlackBerry Enterprise Server mode has changed from STANDBY to PRIMARY. The default is Yes.
Event severity when BlackBerry mode changed to PRIMARY mode.	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server mode has changed to PRIMARY. The default is 15.
Database login	To use SQL authentication, supply login information to access the BlackBerry Enterprise Server database. If left blank, Windows authentication is used. **Note** This information must already be configured in AppManager Security Manager.

Parameter	How to Set It
Mirror database login	To use SQL authentication in a mirrored database environment, supply login information to access the BlackBerry Enterprise Server secondary database. If left blank, Windows authentication is used. **Note** This information must already be configured in AppManager Security Manager.
Raise event if orphaned users exist?	Select **Yes** to raise an event if any orphaned users are found. The default is Yes.
Event severity when orphaned users exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which orphaned users are found. The default is 5.
Monitor number of orphaned users	
Event Notification	
Raise event if number of orphaned users exceeds threshold?	Select **Yes** to raise an event if the number of orphaned users exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of orphaned users	Specify the maximum number of orphaned users that can be found before an event is raised. The default is 10 orphaned users.
Event severity when number of orphaned users exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of orphaned users exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of orphaned users?	Select **Yes** to collect data for charts and reports. If enabled, returns the number of orphaned users on the BlackBerry server. The data details include information about each orphaned user. The default is unselected.

Report_EndToEndResponseTime

Use this Knowledge Script to generate a report about the round-trip response time for an e-mail message. This report includes a measurement of the round-trip response time for a message to travel from a client mailbox, through a selected Exchange Server, to a BlackBerry Enterprise Server handheld device, and for the handheld device to send a response.

This report uses data collected by the ResponseTime Knowledge Script.

Note You may see a gap in data points if this report is run on a BlackBerry Enterprise Server on which the failover status changes from STANDBY to PRIMARY.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Parameter	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval (for example, the average value for 1 hour) • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report Settings	
Include parameter help table?	Select **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Select **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Select **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Select **yes** to append the job ID to the name of the output folder. A job ID is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add timestamp to title?	Select **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event when report succeeds?	Select **yes** to raise an event when the report is successfully generated. The default is yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25.
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_LastUserCount

Use this Knowledge Script to generate a report about the last recorded value for the user count and the percentage of licenses in use for a BlackBerry Enterprise Server. This script uses data collected by the UserCount Knowledge Script.

Note You may see a gap in data points if this report is run on a BlackBerry Enterprise Server on which the failover status changes from STANDBY to PRIMARY.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Report Settings	
Include parameter help table?	Select **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Select **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Select **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Select **yes** to append the job ID to the name of the output folder. A job ID is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.

Parameter	How to Set It
Select properties	Set miscellaneous report properties as needed.
Add timestamp to title?	Select **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event when report succeeds?	Select **yes** to raise an event when the report is successfully generated. The default is yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25.
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_ServerMessageSummary

Use this Knowledge Script to generate a summary of total message traffic on a BlackBerry Enterprise Server during a monitoring interval, including the number of sent, received, and filtered messages.

This report uses data collected by the ServerActivity Knowledge Script.

Note You may see a gap in data points if this report is run on a BlackBerry Enterprise Server on which the failover status changes from STANDBY to PRIMARY.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data Settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report

Parameter	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top *N***: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom *N***: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to yes, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report Settings	
Include parameter help table?	Select **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Select **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Select **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Select **yes** to append the job ID to the name of the output folder. A job ID is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add timestamp to title?	Select **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event when report succeeds?	Select **yes** to raise an event when the report is successfully generated. The default is yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Parameter	How to Set It
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25.
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_SRPConnectivity

Use this Knowledge Script to generate a report about the connectivity (up or down) of the BlackBerry Enterprise Server SRP connection over a specified period.

This report uses data collected by the SRPConnectionStatus Knowledge Script.

Note You may see a gap in data points if this report is run on a BlackBerry Enterprise Server on which the failover status changes from STANDBY to PRIMARY.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Data Settings	
Hours or percentage on chart	Select whether to illustrate availability by hours or by percentage.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top *N***: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom *N***: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to yes, the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Report Settings	

Parameter	How to Set It
Include parameter help table?	Select **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Select **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Select **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Select **yes** to append the job ID to the name of the output folder. A job ID is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add timestamp to title?	Select **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event when report succeeds?	Select **yes** to raise an event when the report is successfully generated. The default is yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25.
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_UserMessageSummary

Use this Knowledge Script to generate a report about the per-user message traffic on a BlackBerry Enterprise Server during a monitoring interval, including the number of sent, received, and filtered messages per user.

This report uses data collected by the UserActivity Knowledge Script.

Note You may see a gap in data points if this report is run on a BlackBerry Enterprise Server on which the failover status changes from STANDBY to PRIMARY.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data Settings	

Parameter	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top *N***: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom *N***: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to yes, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report Settings	
Include parameter help table?	Select **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Select **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Select **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.

Parameter	How to Set It
Add job ID to output folder name?	Select **yes** to append the job ID to the name of the output folder. A job ID is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add timestamp to title?	Select **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event when report succeeds?	Select **yes** to raise an event when the report is successfully generated. The default is yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25.
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

ResponseTime

Use this Knowledge Script to measure the round-trip response time of an e-mail message sent to a BlackBerry handheld device and a response received from the handheld device. Response time is measured using a pair of script iterations. The first time this script runs, the AppManager agent on the selected computer sends a test e-mail message from the mailbox specified in the *Sender Mailbox* parameter to the handheld device by way of the Exchange Server specified in the *Sender Mail Server* parameter.

The test message includes an instruction to the handheld device to send an automated reply. On the second script iteration, the agent checks for the reply and calculates the response time. The BlackBerry Enterprise Server places a timestamp on the message on its way to the handheld device and a timestamp on the reply sent from the handheld device. The agent uses these timestamps to calculate the response time.

This script raises an event if response time exceeds the threshold you set, or if connectivity to the handheld device has been lost.

Prerequisites

The Exchange server specified in the *Sender Mail Server* parameter must have a BES profile on the BES server. In addition, the Exchange server must be associated with a MAPI profile in order to log on and to enable this script to send e-mail to the user account. If the Exchange server has a BES profile, you can run the following utility from the `\AppManager\bin` directory to create the MAPI profile:

```
prof.exe -s servername -m mailboxname - NOTM - p profilename
```

Resource Object

BlackBerry Server

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ResponseTime job fails. The default is 5.
Sender Mailbox (originates test message)	Provide the name of the Exchange mailbox from which the test e-mail message should be sent to the handheld device.
Sender Mail Server (sends test message to handheld)	Provide the name of the Exchange mail server through which the e-mail message should be sent.
SMTP e-mail address of handheld (receives test message)	Provide the e-mail address of the handheld device that will receive the test message through SMTP and reply to it.

Parameter	How to Set It
Delete inactive test messages from Sender's Inbox?	Select **Yes** to remove old test messages used for previous iterations of this job. A test message can become inactive if it will no longer be used to calculate the response time. This may occur if the response time to the handheld device is greater than the job interval length.
Monitor round-trip response time	
Event Notification	
Raise event if round-trip response time exceeds threshold?	Select **Yes** to raise an event if the time taken for the e-mail message to be sent and for a response to be received exceeds the threshold you set. The default is Yes.
Threshold -- Maximum round-trip response time	Specify the maximum number of seconds allowed for the e-mail message to be sent and for a response to be received before an event is raised. Enter a value from 0 to 32000 seconds. The default is 180 seconds.
Event severity when round-trip response time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which response time exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for round-trip response time?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the round-trip response time for the e-mail message. The default is unselected.
Monitor handheld connectivity	
Event Notification	
Raise event if handheld connectivity is down?	Select **Yes** to raise an event if connectivity of the handheld device is down. The default is Yes.
Event severity when handheld connectivity is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which connectivity to the handheld device is lost. The default is 5.
Data Collection	
Collect data for handheld connectivity?	Select **Yes** to collect data for charts and reports. If enabled, returns the up or down status of the handheld device. Returns either: • **0** -- handheld device is down, or • **100** -- handheld device is up. The default is unselected.

ServerActivity

Use this Knowledge Script to monitor activity on a BlackBerry server. This script monitors the number of messages forwarded to handheld devices, received from handheld devices, pending, expired, non-deliverable due to error, and filtered by the server during a monitoring interval. This script also monitors the total number of messages processed during the interval: the sum of the messages forwarded to handheld devices, sent from handheld devices, and filtered.

Resource Object

BlackBerry Server

Default Schedule

The default interval is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ServerActivity job fails. The default is 5.
Database login	To use SQL authentication, supply login information to access the BlackBerry Enterprise Server database. If left blank, Windows authentication is used. **Note** This information must already be configured in AppManager Security Manager.
Mirror database login	To use SQL authentication in a mirrored database environment, supply login information to access the BlackBerry Enterprise Server secondary database. If left blank, Windows authentication is used. **Note** This information must already be configured in AppManager Security Manager.
Blackberry High Availability Notification	
Raise event when BlackBerry STANDBY mode detected?	Select **Yes** to raise an event when the BlackBerry Enterprise Server is in STANDBY mode. The default is unselected.
Event severity when BlackBerry STANDBY mode detected	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server is in STANDBY mode. The default is 15.
Raise event when BlackBerry STANDBY mode changed to PRIMARY mode?	Select **Yes** to raise an event when the BlackBerry Enterprise Server mode has changed from STANDBY to PRIMARY. The default is Yes.
Event severity when BlackBerry mode changed to PRIMARY mode.	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server mode has changed to PRIMARY. The default is 15.
Monitor number of messages forwarded to handhelds	
Event Notification	

Parameter	How to Set It
Raise event if number of messages forwarded to handhelds exceeds threshold?	Select **Yes** to raise an event if the number of messages forwarded to handheld devices exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of messages forwarded to handhelds	Specify the maximum number of messages that can have been forwarded to handheld devices by the monitored server before an event is raised. The default is 10 messages.
Event severity when number of messages forwarded to handhelds exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of forwarded messages exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of messages forwarded to handhelds?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of messages forwarded to handheld devices by the BlackBerry server. The default is unselected.
Monitor number of messages sent from handhelds	
Event Notification	
Raise event if number of messages sent from handhelds exceeds threshold?	Select **Yes** to raise an event if the number of messages sent from handheld device exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of messages sent from handhelds	Specify the maximum number of messages that can have been sent from handheld devices to the BlackBerry server before an event is raised. The default is 10 messages.
Event severity when number of messages sent from handhelds exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of sent messages exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of messages sent from handhelds?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of messages sent from handheld devices to the BlackBerry server. The default is unselected.
Monitor number of messages pending to handhelds	
Event Notification	
Raise event if number of messages pending to handhelds exceeds threshold?	Select **Yes** to raise an event if the number of messages to handheld devices that are pending during the monitoring interval exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of messages pending to handhelds	Specify the maximum number of messages to handheld devices that can be pending before an event is raised. The default is 5 messages.
Event severity when number of messages pending to handhelds exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of pending messages exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for to number of messages pending to handhelds?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of messages pending to handheld devices associated with the monitored server. The default is unselected.
Monitor number of expired messages	
Event Notification	
Raise event if number of expired messages exceeds threshold?	Select **Yes** to raise an event if the number of expired messages exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold -- Maximum number of expired messages	Specify the maximum number of expired messages that can be found on the monitored BlackBerry server before an event is raised. The default is 10 messages.
Event severity when number of expired messages exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of expired messages exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of expired messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of expired messages on the BlackBerry server. The default is unselected.
Monitor number of non-deliverable messages	
Event Notification	
Raise event if number of non-deliverable messages exceeds threshold?	Select **Yes** to raise an event if the number of non-deliverable messages queued at the BlackBerry server exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of non-deliverable messages	Specify the maximum number of non-deliverable messages that can be queued at the BlackBerry server before an event is raised. The default is 5 non-deliverable messages.
Event severity when number of non-deliverable messages exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of non-deliverable messages queued at the BlackBerry server exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of non-deliverable messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of non-deliverable messages queued at the BlackBerry server. The default is unselected.
Monitor number of filtered messages	
Event Notification	
Raise event if number of filtered messages exceeds threshold?	Select **Yes** to raise an event if the number of messages refused by the BlackBerry server exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of filtered messages	Specify the maximum number of messages that can be refused by the BlackBerry server before an event is raised. The default is 10 filtered messages.
Event severity when number of filtered messages exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of refused messages exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of filtered messages?	Select **Yes** to collect data for charts and reports. If enabled, returns the total number of messages refused by the BlackBerry server. The default is unselected.
Monitor total number of messages processed	
Event Notification	
Raise event if total number of messages processed exceeds threshold?	Select **Yes** to raise an event if the total number of messages processed by the BlackBerry server exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold -- Maximum total number of messages processed	Specify the maximum total number of messages that can be processed by the BlackBerry server during any monitoring interval before an event is raised. The default is 50 messages.
Event severity when total number of messages processed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of processed messages exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for total number of messages processed?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of messages processed by the BlackBerry server during the monitoring interval. This total is the sum of the messages forwarded to handheld devices, sent from handheld devices, and filtered. The default is unselected.

ServiceHealth

Use this Knowledge Script to monitor the health of BlackBerry Enterprise Server services. This script monitors the status of services as well as the percentage of server CPU time and the amount of memory used by these services.

The following services are monitored:

- BlackBerry Alert Service
- BlackBerry Controller Service
- BlackBerry Database Consistency Service
- BlackBerry Dispatcher
- BlackBerry Mobile Data Service
  - MDS Connection Service
  - MDS Integration Service
- BlackBerry Policy Service
- BlackBerry Synchronization Service
- BlackBerry Router Service
- BlackBerry Attachment Service
- BlackBerry Administration Service - Application Server
- BlackBerry Administration Service - Native Code Container
- BlackBerry Collaboration Service

This script raises an event if a service is down, or if memory or CPU utilization exceeds either of the thresholds you set.

You can set this script to automatically start a service that is down.

Resource Object

BlackBerry Enterprise Server service

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ServiceHealth job fails. The default is 5.

Parameter	How to Set It
Restart service if down?	Select **Yes** to automatically restart a service that is not running. The default is unselected.
Raise event if attempt to restart service succeeds?	Select **Yes** to raise an event when AppManager successfully restarts a service that is not running. The default is Yes.
Event severity when attempt to restart service succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is successfully restarted. The default is 25.
Raise event if attempt to restart service fails?	Select **Yes** to raise an event when AppManager cannot restart a service that is not running. The default is Yes.
Event severity when attempt to restart service fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service cannot be restarted. The default is 5.
Monitor service status	
Event Notification	
Raise event if service is down?	Select **Yes** to raise an event if a monitored BlackBerry Server service is not running. The default is Yes.
Event severity when service is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service is not running. The default is 5.
Data Collection	
Collect data for service status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the status of all instances of a BlackBerry Server service during the monitoring interval. The default is unselected.
Monitor CPU utilization	
Event Notification	
Raise event if CPU utilization exceeds threshold?	Select **Yes** to raise an event if CPU utilization by BlackBerry Server services exceeds the threshold you set. The default is Yes.
Threshold -- Maximum CPU utilization for BlackBerry Administration Service - Application Server	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the BlackBerry Administration Service - Application Server can have before an event is raised. The default is 30%.
Event severity when CPU utilization for BlackBerry Administration Service - Application Server exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Administration Service Application Server exceeds the CPU utilization threshold. The default is 5.
Threshold -- Maximum CPU utilization for BlackBerry Administration Service - Native Code Container	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the BlackBerry Administration Service - Native Code Container can have before an event is raised. The default is 30%.
Event severity when CPU utilization for BlackBerry Administration Service - Native Code Container exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Administration Service Application Server - Native Code Container exceeds the CPU utilization threshold. The default is 5.

Parameter	How to Set It
Threshold -- Maximum CPU utilization for BlackBerry Alert Service	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the BlackBerry Alert Service can have before an event is raised. The default is 30%.
Event severity when CPU utilization for BlackBerry Alert Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Alert Service exceeds the CPU utilization threshold. The default is 5.
Threshold - Maximum CPU utilization for BlackBerry Attachment Service	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the Attachment Service can have before an event is raised. The default is 30%.
Event severity when CPU utilization for BlackBerry Attachment Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Attachment Service exceeds the CPU utilization threshold. The default is 5.
Threshold - Maximum CPU utilization for BlackBerry Collaboration Service	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the BlackBerry Collaboration Service can have before an event is raised. The default is 30%.
Event severity when CPU utilization for BlackBerry Collaboration Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Collaboration Service exceeds the CPU utilization threshold. The default is 5.
Threshold -- Maximum CPU utilization for BlackBerry Controller Service	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the BlackBerry Controller Service can have before an event is raised. The default is 30%.
Event severity when CPU utilization for BlackBerry Controller Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Controller Server exceeds the CPU utilization threshold. The default is 5.
Threshold -- Maximum CPU utilization for BlackBerry Dispatcher Service	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the BlackBerry Dispatcher Service can have before an event is raised. The default is 30%.
Event severity when CPU utilization for BlackBerry Dispatcher Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Dispatcher Service exceeds the CPU utilization threshold. The default is 5.
Threshold -- Maximum CPU utilization for BlackBerry Database Consistency Service	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the BlackBerry Database Consistency Service can have before an event is raised. The default is 30%.
Event severity when CPU utilization for BlackBerry Database Consistency Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Database Consistency Service exceeds the CPU utilization threshold. The default is 5.
Threshold -- Maximum CPU utilization for BlackBerry MailStore Service	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the BlackBerry MailStore Service can have before an event is raised. The default is 30%.

Parameter	How to Set It
Event severity when CPU utilization for BlackBerry MailStore Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry MailStore Service exceeds the CPU utilization threshold. The default is 5.
Threshold -- Maximum CPU utilization for BlackBerry Mobile Data Service	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the BlackBerry Mobile Data Service can have before an event is raised. The default is 30%.
Event severity when CPU utilization for BlackBerry Mobile Data Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Mobile Data Service exceeds the CPU utilization threshold. The default is 5.
Threshold -- Maximum CPU utilization for BlackBerry Policy Service	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the BlackBerry Policy Service can have before an event is raised. The default is 30%.
Event severity when CPU utilization for BlackBerry Policy Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Policy Service exceeds the CPU utilization threshold. The default is 5.
Threshold -- Maximum CPU utilization for BlackBerry Router Service	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the BlackBerry Router Service can have before an event is raised. The default is 30%.
Event severity when CPU utilization for BlackBerry Router Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Router Service exceeds the CPU utilization threshold. The default is 5.
Threshold -- Maximum CPU utilization for BlackBerry Synchronization Service	Specify the maximum amount of CPU utilization (as a percentage of CPU time) that the BlackBerry Synchronization Service can have before an event is raised. The default is 30%.
Event severity when CPU utilization for BlackBerry Synchronization Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Synchronization Service exceeds the CPU utilization threshold. The default is 5.
Data Collection	
Collect data for CPU utilization?	Select **Yes** to collect data for charts and reports. If enabled, returns the percentage of CPU time used by BlackBerry Enterprise Server services during the monitoring interval. The default is unselected.
Monitor memory utilization	
Event Notification	
Raise event if memory utilization exceeds threshold?	Select **Yes** to raise an event if the memory utilization by BlackBerry server services exceeds the threshold you set. The default is Yes.
Threshold -- Maximum memory utilization for BlackBerry Administration Service - Application Server	Specify the maximum amount of memory that the BlackBerry Administration Service - Application Server can use before an event is raised. The default is 8192 Kilobytes.

Parameter	How to Set It
Event severity when memory utilization for BlackBerry Administration Service - Application Server exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Administration Service - Application Server exceeds the memory utilization threshold. The default is 5.
Threshold -- Maximum memory utilization for BlackBerry Administration Service - Native Code Container	Specify the maximum amount of memory that the BlackBerry Administration Service - Native Code Container can use before an event is raised. The default is 8192 Kilobytes.
Event severity when memory utilization for BlackBerry Administration Service - Native Code Container exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Administration Service - Native Code Container exceeds the memory utilization threshold. The default is 5.
Threshold -- Maximum memory utilization for BlackBerry Alert Service	Specify the maximum amount of memory that the BlackBerry Alert Service can use before an event is raised. The default is 8192 Kilobytes.
Event severity when memory utilization for BlackBerry Alert Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Alert Service exceeds the memory utilization threshold. The default is 5.
Threshold -- Maximum memory utilization for BlackBerry Attachment Service	Specify the maximum amount of memory that the BlackBerry Attachment Service can use before an event is raised. The default is 8192 Kilobytes.
Event severity when memory utilization for BlackBerry Attachment Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Attachment Service exceeds the memory utilization threshold. The default is 5.
Threshold -- Maximum memory utilization for BlackBerry Collaboration Service	Specify the maximum amount of memory that the BlackBerry Collaboration Service can use before an event is raised. The default is 8192 Kilobytes.
Event severity when memory utilization for BlackBerry Collaboration Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Collaboration Service exceeds the memory utilization threshold. The default is 5.
Threshold -- Maximum memory utilization for BlackBerry Controller Service	Specify the maximum amount of memory that the BlackBerry Controller Service can use before an event is raised. The default is 8192 Kilobytes.
Event severity when memory utilization for BlackBerry Controller Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Controller Service exceeds the memory utilization threshold. The default is 5.
Threshold -- Maximum memory utilization for BlackBerry Database Consistency Service	Specify the maximum amount of memory that the BlackBerry Database Consistency Service can use before an event is raised. The default is 8192 Kilobytes.

Parameter	How to Set It
Event severity when memory utilization for BlackBerry Database Consistency Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Database Consistency Service exceeds the memory utilization threshold. The default is 5.
Threshold -- Maximum memory utilization for BlackBerry Dispatcher Service	Specify the maximum amount of memory that the BlackBerry Dispatcher Service can use before an event is raised. The default is 8192 Kilobytes.
Event severity when memory utilization for BlackBerry Dispatcher Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Dispatcher Service exceeds the memory utilization threshold. The default is 5.
Threshold -- Maximum memory utilization for BlackBerry MailStore Service	Specify the maximum amount of memory that the BlackBerry MailStore Service can use before an event is raised. The default is 8192 Kilobytes.
Event severity when memory utilization for BlackBerry MailStore Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry MailStore Service exceeds the memory utilization threshold. The default is 5.
Threshold -- Maximum memory utilization for BlackBerry Mobile Data Service	Specify the maximum amount of memory that the BlackBerry Mobile Data Service can use before an event is raised. The default is 8192 Kilobytes.
Event severity when memory utilization for BlackBerry Mobile Data Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Mobile Data Service exceeds the memory utilization threshold. The default is 5.
Threshold -- Maximum memory utilization for BlackBerry Policy Service	Specify the maximum amount of memory that the BlackBerry Policy Service can use before an event is raised. The default is 8192 Kilobytes.
Event severity when memory utilization for BlackBerry Policy Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Policy Service exceeds the memory utilization threshold. The default is 5.
Threshold -- Maximum memory utilization for BlackBerry Router Service	Specify the maximum amount of memory that the BlackBerry Router Service can use before an event is raised. The default is 8192 Kilobytes.
Event severity when memory utilization for BlackBerry Router Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Router Service exceeds the memory utilization threshold. The default is 5.
Threshold -- Maximum memory utilization for BlackBerry Synchronization Service	Specify the maximum amount of memory that the BlackBerry Synchronization Service can use before an event is raised. The default is 8192 Kilobytes.
Event severity when memory utilization for BlackBerry Synchronization Service exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BlackBerry Synchronization Service exceeds the memory utilization threshold. The default is 5.

Parameter	How to Set It
Data Collection	
Collect data for memory utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of memory used by BlackBerry Enterprise Server services during the monitoring interval. The default is unselected.

SRPConnectionStatus

Use this Knowledge Script to monitor the status of the Server Routing Protocol (SRP) connection between the BlackBerry server and the Research in Motion (RIM) infrastructure.

SRP makes a TCP/IP connection to the wireless network to transmit e-mail messages to and from your wireless ISP. SRP is built on top of a TCP session between Port 3101 of the BlackBerry Enterprise Server and the IP address `srp.blackberry.net` or `srp.na.blackberry.net`.

This script raises an event when the SRP connection is down, and when thresholds are exceeded for the number of failed attempts to reconnect to the wireless network or for the number of seconds the SRP connection can be down during a monitoring interval.

Resource Object

BlackBerry Server

Default Schedule

The default interval is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SRPConnectionStatus job fails. The default is 5.
Raise event if last SRP connection error occurred during last monitoring interval?	Select **Yes** to raise an event if the last SRP connection error that this Knowledge Script detected occurred during the most recent monitoring interval. The default is Yes.
Event severity when last SRP connection error occurred during last monitoring interval	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the last SRP connection error occurred during the most recent monitoring interval. The default is 5.
Blackberry High Availability Notification	
Raise event when BlackBerry STANDBY mode detected?	Select **Yes** to raise an event when the BlackBerry Enterprise Server is in STANDBY mode. The default is unselected.
Event severity when BlackBerry STANDBY mode detected	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server is in STANDBY mode. The default is 15.
Raise event when BlackBerry STANDBY mode changed to PRIMARY mode?	Select **Yes** to raise an event when the BlackBerry Enterprise Server mode has changed from STANDBY to PRIMARY. The default is Yes.

Parameter	How to Set It
Event severity when BlackBerry mode changed to PRIMARY mode.	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server mode has changed to PRIMARY. The default is 15.
Monitor SRP connection status	
Event Notification	
Raise event if SRP connection is down?	Select **Yes** to raise an event if the SRP connection to the RIM wireless network is down. The default is Yes.
Event severity when SRP connection is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SRP connection is down. The default is 5.
Data Collection	
Collect data for SRP connection status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the status of the SRP connection to the wireless network, either: • 0 -- SRP connection is down, or • 100 -- SRP connection is up. The default is unselected.
Monitor number of failed SRP reconnects	
Event Notification	
Raise event if number of failed SRP reconnects exceeds threshold?	Select **Yes** to raise an event if the number of failed attempts to re-establish the SRP connection exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of failed SRP reconnects	Specify the maximum number of times that an attempt to re-establish a lost SRP connection to the wireless network can fail before an event is raised. The default is 2 times.
Event severity when number of failed SRP reconnects exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event if the number of attempts to re-establish a connection exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of failed SRP reconnects?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times that an attempt to re-establish a lost SRP connection to the wireless network failed during the monitoring interval. The default is unselected.
Monitor number of seconds not connected to wireless network	
Event Notification	
Raise event if number of seconds not connected to wireless network exceeds threshold?	Select **Yes** to raise an event if the number of seconds that the SRP connection to the RIM wireless network was down exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of seconds not connected to wireless network	Specify the maximum number of seconds that the BlackBerry Enterprise Server was not connected to the wireless network because the SRP connection was down. If the threshold is exceeded, an event is raised. The default is 30 seconds.
Event severity when number of seconds not connected to wireless network exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event if the length of time the BlackBerry Enterprise Server was down exceeds the threshold you set. The default is 5.

Parameter	How to Set It
Data Collection	
Collect data for number of seconds not connected to wireless network?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of time, in seconds, that the SRP connection to the RIM wireless network was down during the monitoring interval. The default is unselected.

SRPTest

Use this Knowledge Script to perform a Ping test of the Server Routing Protocol (SRP) connection between the BlackBerry server and the Research In Motion (RIM) wireless network.

SRP makes a TCP/IP connection to the wireless network to transmit e-mail messages to and from the wireless ISP. SRP is built on top of a TCP session between the BlackBerry Enterprise Server and an IP address.

An event is raised when the BlackBerry server SRP connection returns a non-zero exit code (meaning that a connection could not be established). The script can also raise an event if the Ping test is successful.

Note
This script requires the BBSRPTest utility to run. If it is not installed in the default location, you need to supply a full path to its location.

Resource Object

BlackBerry Enterprise Server

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SRPTest job fails. The default is 5.
Path and filename for BBSRPTest utility	Provide the path and filename for the BlackBerry utility required to run the Ping test. Leave blank to use the BlackBerry default path.
BBSRPTest utility timeout	Set a timeout value from 1 to 120 seconds. The script tries to locate the `BBSRPTest` utility (required to run the Ping test) until the timeout expires. The default is 20 seconds.
Raise event if Ping test succeeds?	Select **Yes** to raise an event if the Ping test to the BlackBerry server SRP connection is successful. The default is Yes.
Event severity when Ping test succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Ping test was successful. The default is 25.
Raise event if Ping test fails?	Select **Yes** to raise an event if the Ping test to the BlackBerry server SRP connection returns a non-zero exit code. The default is Yes.
Event severity when Ping test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Ping test returns a non-zero exit code. The default is 5.
Monitor SRP Ping status	

Parameter	How to Set It
Data Collection	
Collect data for SRP Ping status?	Select **Yes** to collect data for charts and reports. If enabled, returns the following: • 100 -- SRP Ping test was successful • 0 -- SRP Ping test failed. The default is unselected.

UserActivity

Use this Knowledge Script to monitor the activity of each user on a BlackBerry server. This script monitors, on a per-user basis, the number of messages forwarded to handheld devices, received from handheld devices, pending, expired, non-deliverable due to error, and filtered by the server during a monitoring interval. This script also monitors the total number of messages processed during the interval.

This script raises an event if a metric exceeds one of the thresholds you set.

If you have supplied a valid filename for the *File with list of users to monitor* parameter and you make any changes to that file, the changes will not take effect for that job. Nor can you start and stop the running job for the changes to take effect. You must instead create a new job using the modified file, because the file is read only when the UserActivity job is created. The values in the file are not updated until a new job is created.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the UserActivity job fails. The default is 5.
Database login	To use SQL authentication, supply login information to access the BlackBerry Enterprise Server database. If left blank, Windows authentication is used. **Note** SQL authentication information must already be configured in AppManager Security Manager.
Mirror database login	To use SQL authentication in a mirrored database environment, supply login information to access the BlackBerry Enterprise Server secondary database. If left blank, Windows authentication is used. **Note** This information must already be configured in AppManager Security Manager.
Maximum number of users to record data streams for	Specify the maximum number of users to include when collecting data. When data collection is enabled, this script returns per-user statistics for each user on the server. This parameter sets an upper limit on the number of users for whom such data should be collected and returned. The default is 50 users.

Parameter	How to Set It
File with list of users to monitor	Click **Browse** (...) to locate a file containing a list of the users you want to monitor with this script. The file should contain a list of the user names associated with the email accounts whose results you want to include in the event details. Separate each user name with a pipe (|).
Blackberry High Availability Notification	
Raise event when BlackBerry STANDBY mode detected?	Select **Yes** to raise an event when the BlackBerry Enterprise Server is in STANDBY mode. The default is unselected.
Event severity when BlackBerry STANDBY mode detected	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server is in STANDBY mode. The default is 15.
Raise event when BlackBerry STANDBY mode changed to PRIMARY mode?	Select **Yes** to raise an event when the BlackBerry Enterprise Server mode has changed from STANDBY to PRIMARY. The default is Yes.
Event severity when BlackBerry mode changed to PRIMARY mode.	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server mode has changed to PRIMARY. The default is 15.
Monitor number of messages forwarded to handheld	
Event Notification	
Raise event if number of messages forwarded to handheld exceeds threshold?	Select **Yes** to raise an event if the number of messages forwarded to any handheld device by the monitored server exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of messages forwarded to handheld	Specify the maximum number of messages that can be forwarded to any handheld device by the monitored server before an event is raised. The default is 10 messages.
Event severity when number of messages forwarded to handheld exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of forwarded messages exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of messages forwarded to handheld?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of messages forwarded to each handheld device by the monitored server. The default is unselected.
Monitor number of messages sent from handheld	
Event Notification	
Raise event if number of messages sent from handheld exceeds threshold?	Select **Yes** to raise an event if the number of messages sent from any handheld device exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of messages sent from handheld	Specify the maximum number of messages that can be sent from a handheld device to the BlackBerry Enterprise Server before an event is raised. The default is 10 messages.
Event severity when number of messages sent from handheld exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of sent messages exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of messages sent from handheld?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of messages sent from each handheld device to the BlackBerry Enterprise Server. The default is unselected.

Parameter	How to Set It
Monitor number of messages pending to handheld	
Event Notification	
Raise event if number of messages pending to handheld exceeds threshold?	Select **Yes** to raise an event if the number of messages to any handheld device that are pending during the monitoring interval exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of messages pending to handheld	Specify the maximum number of messages to any handheld device that can be pending before an event is raised. The default is 5 messages.
Event severity when number of messages pending to handheld exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of pending messages exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for to number of messages pending to handheld?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of messages pending to each handheld device associated with the monitored server. The default is unselected.
Monitor number of expired messages	
Event Notification	
Raise event if number of expired messages exceeds threshold?	Select **Yes** to raise an event if the number of expired messages for any user exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of expired messages	Specify the maximum number of expired messages for any user that can be found on the monitored server before an event is raised. The default is 10 messages.
Event severity when number of expired messages exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of expired messages exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of expired messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of expired messages for each user on the monitored server. The default is unselected.
Monitor number of non-deliverable messages	
Event Notification	
Raise event if number of non-deliverable messages exceeds threshold?	Select **Yes** to raise an event if the number of undeliverable messages for any user on the monitored server exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of non-deliverable messages	Specify the maximum number of undeliverable messages that can be found for any user on the BlackBerry Enterprise Server before an event is raised. The default is 5 undeliverable messages.
Event severity when number of non-deliverable messages exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of undeliverable messages exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of non-deliverable messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of undeliverable messages per user on the monitored server. The default is unselected.
Monitor number of filtered messages	
Event Notification	

Parameter	How to Set It
Raise event if number of filtered messages exceeds threshold?	Select **Yes** to raise an event if the number of messages for a user that were refused by the monitored server exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of filtered messages	Specify the maximum number of messages for any user that can be refused by the monitored server before an event is raised. The default is 10 filtered messages.
Event severity when number of filtered messages exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of refused messages exceeds the threshold you set. the default is 5.
Data Collection	
Collect data for number of filtered messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of messages for each user that were refused by the monitored server. The default is unselected.
Monitor total number of messages processed	
Event Notification	
Raise event if total number of messages processed exceeds threshold?	Select **Yes** to raise an event if the number of messages for any user that can be processed by the monitored server exceeds the threshold you set. The default is Yes.
Threshold -- Maximum total number of messages processed	Specify the maximum number of messages for any user that can be processed by the monitored server during any monitoring interval before an event is raised. The default is 50 messages.
Event severity when total number of messages processed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of processed messages exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for total number of messages processed?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of messages for each user that were processed by the BlackBerry Enterprise Server during the monitoring interval. This total is the sum of the messages forwarded to handheld devices, sent from handheld devices, and filtered, on a per-user basis. The default is unselected.

UserCount

Use this Knowledge Script to report the total number of users and the percentage of licenses in use on a BlackBerry Enterprise Server.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the UserCount job fails. The default is 5.
Blackberry High Availability Notification	
Raise event when BlackBerry STANDBY mode detected?	Select **Yes** to raise an event when the BlackBerry Enterprise Server is in STANDBY mode. The default is unselected.
Event severity when BlackBerry STANDBY mode detected	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server is in STANDBY mode. The default is 15.
Raise event when BlackBerry STANDBY mode changed to PRIMARY mode?	Select **Yes** to raise an event when the BlackBerry Enterprise Server mode has changed from STANDBY to PRIMARY. The default is Yes.
Event severity when BlackBerry mode changed to PRIMARY mode.	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server mode has changed to PRIMARY. The default is 15.
Monitor number of users on a BlackBerry server	
Event Notification	
Raise event if number of users on a BlackBerry server exceeds threshold?	Select **Yes** to raise an event if the number of users associated with a BlackBerry server exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of users on a BlackBerry server	Specify the maximum number of users that can be associated with a BlackBerry server before an event is raised. The default is 1900 users.
Event severity when number of users on a BlackBerry server exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of users exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of users on a BlackBerry server?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of users associated with the BlackBerry server. The default is unselected.

Parameter	How to Set It
Monitor percentage of licenses in use	
Event Notification	
Raise event if percentage of licenses in use exceeds threshold?	Select **Yes** to raise an event if the percentage of BlackBerry Enterprise Server licenses currently in use exceeds the threshold you set. The default is Yes.
Threshold -- Maximum percentage of licenses in use	Specify the maximum percentage of BlackBerry Enterprise Server licenses that can be in use before an event is raised. The default is 80%.
Event severity when percentage of licences in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of licenses in use exceeds the threshold. The default is 5.
Data Collection	
Collect data for percentage of licences in use?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of BlackBerry Enterprise Server licenses that are currently being used. The default is unselected.

UsersWithPendingMessages

Use this Knowledge Script to report on the percentage of all users whose handheld device accounts contain pending messages on a BlackBerry Enterprise Server. You can specify which users to monitor and can set a threshold for the maximum percentage of users with pending messages allowed on that server.

Any changes you make to the file specified in the *File with list of users to monitor* parameter while the job is running do not take effect for that job. Nor will the changes take effect if you start and stop the running job. You must instead create a new job using the modified file. Because the file is read-only when the UsersWithPendingMessages job is created, the values in the file are not updated until a new job is created.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the UsersWithPendingMessages job fails. The default is 5.
Database login	To use SQL authentication, supply login information to access the BlackBerry Enterprise Server database. If left blank, Windows authentication is used. **Note** This information must already be configured in AppManager Security Manager.
Mirror database login	To use SQL authentication in a mirrored database environment, supply login information to access the BlackBerry Enterprise Server secondary database. If left blank, Windows authentication is used. **Note** This information must already be configured in AppManager Security Manager.
File with list of users to monitor	Click **Browse** (...) to locate a file containing a list of the handheld device users you want to monitor with this script. The file should list the display names associated with the email accounts whose results you want to include in the event details. Place each display name on a separate line in the file.
Blackberry High Availability Notification	
Raise event when BlackBerry STANDBY mode detected?	Select **Yes** to raise an event when the BlackBerry Enterprise Server is in STANDBY mode. The default is unselected.
Event severity when BlackBerry STANDBY mode detected	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server is in STANDBY mode. The default is 15.

Parameter	How to Set It
Raise event when BlackBerry STANDBY mode changed to PRIMARY mode?	Select **Yes** to raise an event when the BlackBerry Enterprise Server mode has changed from STANDBY to PRIMARY. The default is Yes.
Event severity when BlackBerry mode changed to PRIMARY mode.	Set the severity level from 1 to 40 to indicate the importance of an event in which the BlackBerry Enterprise Server mode has changed to PRIMARY. The default is 15.
Monitor percentage of users with messages pending to handheld?	Select **Yes** to monitor the percentage of users on a BlackBerry server who can have messages pending and not yet sent to their handheld device. The default is Yes.
Event Notification	
Raise event if percentage of users with messages pending to handheld exceeds threshold?	Select **Yes** to raise an event if the percentage of users with messages pending and not yet sent to their handheld device exceeds the threshold you set. The default is Yes.
Threshold -- Maximum percentage of users with messages pending to handheld	Specify the maximum percentage of users associated with a BlackBerry server that can have messages pending before an event is raised. The default is 15%.
Event severity when percentage of users with messages pending to handheld exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Data Collection	
Collect data for percentage of users with messages pending to handheld?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of users associated with the BlackBerry server. The default is unselected.

Chapter 15
BlackBerry Knowledge Scripts

The BlackBerry category provides the following Knowledge Scripts for monitoring BlackBerry servers. It also includes Knowledge Scripts to create reports about the performance of your BlackBerry Enterprise Server implementation.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
BesAlertForward	Sends alerts using SNMP, MAPI Mail, Notes Mail, Pager, MessageBox, or a customized method whenever an event of a specified type occurs.
DebugLogTotalSize	Calculates the total debug log size.
EventLog	Monitors and filters information in the Windows Event Log specific to the BlackBerry Enterprise Server.
ExchangeAvail	Checks Exchange Server availability and the response time for a client request to open a mailbox.
HungThreads	Monitors a BlackBerry Server service for hung (blocked) threads. Can optionally restart a service.
MessagingServerList	Lists all Exchange Servers with at least one user on the BlackBerry Enterprise Server.
MsgAvgSize	Gathers average size in bytes of messages transferred to handheld devices by a BlackBerry Server.
MsgBytesReceived	Gathers the number of message bytes transferred to a handheld device during a monitoring interval.
MsgsExpired	Monitors the number of messages that expired during the monitoring interval.
PurgeDebugLog	Monitors the total size of BlackBerry Server service debug log files and optionally deletes files that are older than a specified date.
Report_EndToEndConnectivity	Generates a report about connectivity between the Exchange and BlackBerry Enterprise Servers and a BlackBerry handheld.
Report_EndToEndResponseTime	Generates a report about email round-trip response time.
Report_ExchangeConnectionTime	Generates a report about the response time of an Exchange Server.
Report_ExchangeConnectivity	Generates a report about connectivity with an Exchange Server.

Knowledge Script	What It Does
Report_MessagesByInterval	Generates a report about the total number of messages exchanged during a monitoring interval.
Report_MessageSummary	Generates a report about the total number of new messages, including messages sent, received, filtered, and queued during the monitoring interval.
Report_ServerList	Generates a report listing the messaging (Exchange) servers used by a BlackBerry Server service.
Report_SRPConnectionUptime	Generates a report about the percentage of uptime for the connection to the wireless network.
Report_SRPConnectivity	Generates a report about the connectivity (up or down) of the BlackBerry Server SRP connection over a specified period.
Report_UserByServer	Generates a report about the number of users on an Exchange Server for a BlackBerry Server.
Report_UserListing	Generates a report about the number of users on a BlackBerry Server service. A list of users can be sorted by server association or alphabetically.
ResponseTime	Sends a message to a handheld from the BlackBerry-enabled Exchange mailbox, checks for a reply, and determines end-to-end response time.
ServerHealth	Monitors BlackBerry Enterprise Server health, the percentage of memory used, and the percentage of CPU and memory used by BlackBerry Server processes.
ServerLoad	Monitors the rate at which messages are filtered, sent, received, queued and the total new message activity during an interval.
ServicesDown	Monitors the availability of BlackBerry Enterprise Server services and optionally restarts a service.
SNMPAlertForward	Monitors and filters information in the Windows EventLog and sends alerts as SNMP messages.
SRPConnectionStatus	Monitors the percentage of uptime during a specified interval for the Server Routing Protocol (SRP) connection between the BlackBerry Enterprise Server and the Research in Motion (RIM) infrastructure.
SRPTest	Performs a test of the SRP connection to make sure the wireless network can be reached.
UserCountByServer	Lists the number of users on a BlackBerry Server and includes each user's association with a messaging (Exchange) server.
UserList	Lists the users on a BlackBerry Server, plus the total number of users on the BlackBerry Enterprise Server.

BesAlertForward

Use this Knowledge Script to send alerts using SNMP, MAPI Mail, Notes Mail, Pager, MessageBox, or another customized method whenever an event of a specified type occurs. Using this script, you can track Windows Event Log entries that match a filtering criterion.

Resource Object

BlackBerry Enterprise Server

Default Schedule

The default schedule is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed

Description	How to Set It
Raise event if matching event log entries found?	Set to **y** to raise events and send an alert. Default is y.
Collect data for event log entries?	Set to **y** to collect data for charts and reports. If set to y, returns the Event Log entries that matched your search criteria. Default is n.
Separate event data from different sources into multiple events?	Set to **y** to separate event entries from the different log files into different data streams. If you accept the default, n, all the event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. For example, if you are monitoring both the System and Application logs, you may want to set this parameter to **y** so that events in the System log are tracked separately from events in the Application log. Default is n.
Filter by log source: • System • Security • Application	Specify the event log you want to monitor. You can specify multiple event logs separated by commas. For example, `System,Security,Application`. Default is `Application`.
Filter by event type: • Error • Warning • Information • Success Audit • Failure Audit	Set to **y** to monitor each type of event log entry. The default is y.
Filter by event source	Enter a string to direct the Knowledge Script to monitor events generated by a particular source, such as SQLExecutive, SNMP, or the Service Control Manager. The script looks for matching entries in the Event Log's **Source** field. You can enter multiple strings separated by commas and include or exclude criteria using a colon (:). If you are only specifying include criteria, the colon is not necessary. The default value is `BlackBerry`.

Description	How to Set It
Filter by event category	If you are interested in events in a particular category such as, Server or Logon, enter an appropriate search string. The Knowledge Script looks for matching entries in the Event Log category field. You can enter multiple strings separated by commas and include or exclude criteria using a colon (:). If you are only specifying include criteria, the colon is not necessary.
Filter by event ID	If you are interested in particular event IDs, enter an appropriate search string or event ID range. For example, 100-2000. The Knowledge Script looks for matching entries in the Event Log's **Event** field. You can enter multiple IDs and ranges separated by commas. For example: `1,2, 10-15, 202` You can also include or exclude criteria using a colon (:). If you are only specifying include criteria, the colon is not necessary.
Filter by user	If you are interested in events associated with a particular user, enter an appropriate search string. For example, *DomainName**UserName*. The Knowledge Script looks for matching entries in the Event Log's **User** field. You can enter multiple strings separated by commas and include or exclude criteria using a colon (:). If you are only specifying include criteria, the colon is not necessary.
Filter by computer	If you are interested in events associated with a particular computer, enter an appropriate search string. The Knowledge Script looks for matching entries in the Event Log's **Computer** field. You can enter multiple strings separated by commas and include or exclude criteria using a colon (:). If you are only specifying include criteria, the colon is not necessary.
Filter by event description	If you are interested in events with a particular detail description, enter an appropriate search string. The Knowledge Script looks for matching entries in the Event Log's **Description** field. You can enter multiple strings separated by commas and include or exclude criteria using a colon (:). If you are only specifying include criteria, the colon is not necessary.
Maximum number of log entries per event	Specify the maximum number of entries to be recorded into each event detail message. If the Knowledge Script finds more entries from the log than can be placed in one event message, it returns multiple events to report all the outstanding entries in the log. The default is 30 entries.
Event severity when matching event log entries found	Set the event notification level to show the visibility for the event. The default severity level is 8. You may want to adjust the severity depending on which log or type of event you are checking for.

Example of How This Script is Used

The following is an example of how you can customize this script for your environment. For example, to detect security failures among the general system events, set the following options:

Properties and Parameters	Values for Detecting Security Failures
Schedule interval	Every 10 minutes
Event	y
Log	Security
Type	FailureAudit

Properties and Parameters	Values for Detecting Security Failures
Severity	2
Action	MapiMail

On the **Values** tab, set the "Event" parameter to **y** indicating that an event is generated anytime the conditions are met, and set "Log" and "Type" to "Security" and "FailureAudit" indicating this to be a very serious and highly visible event. Leave the other filtering options blank.

On the **Actions** tab, indicate that an email message should be sent if an event is raised. AppManager checks for security failures and notifies a designated recipient with an email message if a security failure occurs.

Here is another example. To detect problems with a SQL Server, you can set the following options:

Properties and Parameters	Values for Detecting Security Failures
Schedule interval	30 minutes
Event?	y
Log	Application
Type	Error
Source	MSSQLServer
Severity	8
Action	MapiMail

You may want to collect data and graph a trend chart from your System Event Log. Here is how to set the other parameters:

Properties and Parameters	Values for Detecting Security Failures
Schedule interval	1 hour
Event?	y
Log	System
All other filters	not set
Action	null

View the first batch of filtered results in the detailed data message when you double-click a datapoint. Additional matching entries may be included in the graph.

DebugLogTotalSize

Use this Knowledge Script to calculate the total size of the local debug logs. If you choose to collect data, this Knowledge Script returns the number of MB of hard disk space used by the daily `debuglogYYYYMMDD.txt` files. An event is raised if the threshold you set for debug log size is exceeded.

Note
You may want to periodically use the PurgeDebugLogKnowledge Script to purge the debug log file.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise an event when the size of the local debug log exceeds the threshold. Default is y.
Collect data for debug log file size (MB)?	Set to **y** to collect data for charts and reports. If set to **y**, returns the size of the local debug log in MB. Default is n.
Maximum event threshold for debug log file size	Enter the maximum event threshold for debug log file size. Enter a value from 0 to 32000 MB. Default is 1000 MB.
Event severity level when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event when monitoring fails. Enter a value from 1 to 40. Default is 5.

EventLog

Use this Knowledge Script to monitor information specific to the BlackBerry Enterprise Server that appears in the Windows Event Log. This script periodically scans the Windows Event Log for BlackBerry Enterprise Server service entries and raises an event if any are found. The event details specify the type of event that occurred.

If data is collected, this script returns the number of Blackberry-related events in the Windows Event Log.

Resource Object

BlackBerry Enterprise Server

Default Schedule

The default schedule is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if log entries found?	Set to **y** to raise events when this Knowledge Script discovers BlackBerry Enterprise Server service entries in the Windows Event Log. Default is y.
Collect data for number and type of events found?	Set to **y** to collect data for charts and reports. If set to **y**, returns the number of new Event Log entries. Default is n.
Maximum number of log entries per event	Enter the maximum number of entries per event report. Enter a value from 1 to 100 entries. Default is 30 entries.
Event severity level when log entries found	Set the event severity level, from 1 to 40, to indicate the importance of the event. Adjust the severity depending on the types of events you are checking for. Default severity level is 8.

Example of How This Script is Used

Let us assume you ran this Knowledge Script once. The event details indicate that a `MAPI_E_LOGON` event occurred during the monitoring interval. This event indicates that the BlackBerry Enterprise Server cannot log on to the Exchange Server MAPI. You can then proceed to resolve the problem by re-establishing the MAPI connection so that the BlackBerry Enterprise Server service can send mail to the user.

ExchangeAvail

Use this Knowledge Script to measure the time taken to log on to the Exchange Server, and to check whether the Exchange Server is available.

This script also checks Exchange Server response time by measuring its response to a client request to open a mailbox. The script opens a selected mailbox on the Exchange Server to determine the availability of the BlackBerry Enterprise Server to the Exchange Link. This script then opens up a MAPI session to test whether the Exchange Server responds. The time taken to log on to the Exchange Server is recorded as the data stream used for the Report_ExchangeConnectivity report.

Specify a corresponding mailbox for each Exchange Server monitored. If an Exchange service is not accessible, an event is raised.

Resource Object

BlackBerry Enterprise Server

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if server unavailable or if threshold exceeded?	Set to **y** to raise an event if the Exchange Server is unavailable or if threshold is exceeded. The default is y.
Collect data for availability, response time, and connection time?	Set to **y** to collect data for charts and reports. If set to **y**, returns data about the availability, response and connection time of the selected Exchange Server(s).The default is y.
List of Exchange Servers	Create a list of Exchange Servers to monitor. Separate server names with ",". Default is "`Exchange_Server1`".
List of Exchange mailboxes	Create a list of the Exchange mailboxes to monitor. Separate mailbox names with ",". Default is "`Mailbox1`".
Full path to file with list of Exchange Servers and mailboxes	Enter a fully qualified path to a file containing a list of Exchange Server--Exchange mailbox pairs to monitor. Use the following format for the list: `Server name,Mailbox name`. Use commas to separate server and mailbox names. Each line in the file must contain a different server-mailbox pair.
Threshold -- Maximum response time	Enter the maximum threshold, in seconds, for a response from: • Exchange Server • Exchange mailbox Enter a value from 0 to 100 seconds. Default is 60 seconds.
Number of messages to retrieve to test response time.	Enter the number of messages to retrieve to determine the response time. Enter a value from 1 to 32,000 messages. Default is 10 messages.
Event severity when server unavailable or when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event for monitoring failure. Default is 8.

HungThreads

Use this Knowledge Script to monitor a BlackBerry Server service for "hung" threads. Hung threads decrease the number of requests that can be concurrently processed by the service. Any thread that starts and then does not finish is considered "hung."

Note
If you are using BlackBerry Enterprise Server version 2.1, you may be familiar with the term "blocked" threads, rather than "hung" threads. Both terms mean the same thing. In this guide, we use the term hung threads.

This Knowledge Script waits for a specified number of cycles before raising an event to see if the hung threads become unblocked. This waiting period is referred to as the "wait count."

An event is raised only when both the number of hung threads and the wait count, in cycles, exceed the specified thresholds. You also have the option to restart the hung service automatically. If you choose to collect data, this script returns data about the number of hung threads, the thread ID, and the wait count.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if threshold and wait count exceeded?	Set to **y** to raise events when the number of hung threads exceeds the threshold and wait count is exceeded. Default is y.
Collect data for hung threads, thread ID, and wait count?	Set to **y** to collect data for charts and reports. Default is n. If set to **y**, returns data about hung threads, including the thread ID and wait count.
Wait count	Set a wait count for each hung thread. The Knowledge Script waits the specified number of cycles to detect whether hung threads become unblocked. Default is 2 cycles.
Threshold -- Maximum number of hung threads	Enter the maximum number of hung threads allowed. Enter a value from 1 to 100. Default is 1 thread.
Restart service if down?	Set to **y** to automatically restart a BlackBerry server service that is hung. Default is y.
Event severity for restart failure	Set the severity level, from 1 to 40, to indicate the importance if an attempt to restart a hung service failed. Default is 5.
Event severity for restart success	Set the severity level, from 1 to 40, to indicate the importance if an attempt to restart a hung service succeeded. Default is 25.
Event severity if restart disabled	Set the severity level, from 1 to 40, to indicate the importance if the "Restart service if down?" parameter is set to n. Default is 18.

MessagingServerList

Use this Knowledge Script to report the number of different Exchange Servers interacting with a BlackBerry Server service. Each Exchange Server must have at least one user on the BlackBerry Server.

An event is raised if the total number of messaging servers exceeds the threshold.

To ensure that this Knowledge Script works properly, check to make sure that the `BBUserAdminService` is running.

Note
This Knowledge Script requires the BBUserAdminClient executable to run. To ensure that this Knowledge Script works properly, first check to make sure that the BBUserAdminService is running.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every week**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event on script success?	Set to **y** to raise an event if the job succeeds. Default is n.
Raise event if threshold exceeded?	Set to **y** to raise an event if the total number of messaging servers exceeds the threshold. Default is y.
Collect data for number of messaging servers?	Set to **y** to collect data for charts and reports. If set to **y**, returns the number of messaging servers for the selected BlackBerry Server service. Default is y.
Threshold -- Maximum number of messaging servers	Enter the maximum number of different messaging servers that can be found for a single BlackBerry Server service before an event is raised. Default is 12 servers.
Path and filename for BBuserAdminClient executable	Enter the path and filename where the file `BBUserAdminClient.exe` is installed. Leave blank to accept the default path.
`BBUserAdminClient` executable timeout	Set a timeout value to determine how long the script attempts to reach the `BBUserAdminClient` executable. Enter a value from 1 to 120 seconds. Default is 10 seconds.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the threshold-crossing event. Default is 25.

MsgAvgSize

Use this Knowledge Script to find the average message size in KB, of the messages transferred to handhelds by a BlackBerry Server during the monitoring interval. This script considers email messages and calendar entries in its calculations. An event is raised if the average message size exceeds the threshold you set.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise an event if the average message size exceeds the threshold. Default is y.
Collect data for average message size?	Set to **y** to collect data for charts and reports. If set to **y**, returns the average message size of the messages transferred to handhelds during the monitoring interval. Default is n.
Threshold -- Maximum average message size	Enter the maximum threshold for the average message size. Default is 2 KB.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the threshold-crossing event. Default is 25.

MsgBytesReceived

Use this Knowledge Script to gather the total bytes received by handhelds per interval. This script does not consider bytes sent, but does consider calendar entries.

An event is raised when the threshold for total bytes received by handhelds is exceeded. If data is collected, the average number of bytes received by handhelds during the monitoring interval is returned.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise an event if the total bytes received by handhelds during the monitoring interval exceeds the threshold. Default is y.
Collect data for number of bytes transferred?	Set to **y** to collect data for charts and reports. If set to **y**, returns the average number of bytes received by handhelds during the monitoring interval. Default is n.
Threshold -- Maximum bytes transferred	Enter the maximum number of bytes that can be received by handhelds before an event is raised. Default is 500 KB.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the threshold-crossing event. Default is 25.

MsgsExpired

Use this Knowledge Script to monitor the number of messages that expired during the monitoring interval. A message intended for a BlackBerry handheld expires if seven days passes before it can be sent. For example, the handheld is turned off.

Resource Object

BlackBerry Enterprise Server

Default Schedule

The default schedule is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise an event if the number of expired messages exceeds the threshold. Default is y.
Collect data for number of expired messages?	Set to **y** to collect the number of expired messages per interval. Default is n.
Threshold -- Maximum number of expired messages	Enter the maximum total number of expired messages that can occur before an event is raised. Default is 50.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 8.

PurgeDebugLog

Use this Knowledge Script to monitor the total size of BlackBerry Enterprise Server debug log files. This script can be set to automatically purge a debug log, but only when a log exceeds both thresholds, for log file size and log age. An event is raised if either threshold is crossed.

Note
For a BlackBerry Enterprise Server with average load and an average number of users, the average debug log file size per day is estimated at 100 MB. The default threshold for log age (180 days) is based on having six months' worth of debug log data before starting the auto-purge.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event for total debug log file size?	Set to **y** to raise events when the total debug log file size exceeds threshold. Default is y.
Collect data for total debug log file size?	Set to **y** to collect data for charts and reports. If set to **y**, returns the total size (GB) and age (days) of the debug log. Default is n.
Threshold -- Maximum total debug log file size	Enter the maximum total debug log file size (MB) allowed before an event is raised. Enter a value from 0 to 32000 MB. Default is 1000 MB.
Automatically purge debug log files?	Set to **y** to automatically purge the debug log file when both purge thresholds are exceeded. Default is y.
Purge threshold -- Maximum total debug log file size	Enter the maximum total debug log file size allowed before log is purged. Enter a value from 0 to 1000 GB. Default is 18 GB.
Purge threshold -- Maximum debug log file age	Enter the maximum debug log file age, in days, allowed before the log is purged. Enter a value from 0 to 1000 days. Default is 180 days.
Raise event when debug log successfully purged?	Set to **y** to raise events when the debug log file is successfully purged. Default is y.
Collect data for number of debug log files purged and filenames?	Set to **y** to collect data for charts and events about the number of purged debug log files and their filenames. Default is n.
Event severity when log file size threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event when monitoring fails. Default is 8.
Event severity when debug log file purged	Set the event severity level, from 1 to 40, to indicate the importance of the event when a log is deleted. Default is 35.

Report_EndToEndConnectivity

Use this Knowledge Script to generate a report about the connectivity between the Exchange and BlackBerry Enterprise Servers and a BlackBerry handheld. This report allows you to make a statistical analysis of the data point values. For example, the average or maximum value over a time period.

This report uses data collected by the ResponseTime Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Data settings	Use the following parameters to define the statistical calculation applied to data, and which of the data is displayed.
Hours or percentage on chart	Select whether to illustrate availability by hours or by percentage.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value that is, lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top *N***: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom *N***: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. Default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. Default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.

Description	How to Set It
Include parameter help card?	Set to yes to include a table in the report that lists parameter settings for the report script. Default is yes.
Include table?	Set to yes to include a table of data stream values in the report. Default is yes.
Include chart?	Set to yes to include a chart of data stream values in the report. Default is yes.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to yes to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. Default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to yes to raise an event when the report is successfully generated. Default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_EndToEndResponseTime

Use this Knowledge Script to generate a report about Exchange Server response time. This report includes a measurement of the round-trip response time for a message to travel from a client mailbox, via a selected Exchange Server, to a BlackBerry Enterprise Server handheld, and for the handheld to send a response.

This report uses data collected by the ResponseTime Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers. Each page shows all the data streams collected from a single computer. • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers. For example, each page shows the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to yes to include a table in the report that lists parameter settings for the report script. Default is yes.
Include table?	Set to yes to include a table of data stream values in the report. Default is yes.
Include chart?	Set to yes to include a chart of data stream values in the report. Default is yes.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to yes to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. Default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to yes to raise an event when the report is successfully generated. Default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_ExchangeConnectionTime

Use this Knowledge Script to generate a report about the response time of Exchange services. This report measures the time taken to log on to the Exchange Server and helps make a statistical analysis of the data point values. For example, you can get the average or maximum value over a time period.

The ExchangeAvail Knowledge Script opens up a MAPI session to the Exchange Server to check availability. The script records the time taken to log on to the Exchange Server and uses this data stream to generate the report.

Resource Object

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers. Each page shows all the data streams collected from a single computer. • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers. For example, each page shows the value of the *NT_CpuResource-All Threads(#)* data stream from each computer. • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to yes to include a table in the report that lists parameter settings for the report script. Default is yes.
Include table?	Set to yes to include a table of data stream values in the report. Default is yes.
Include chart?	Set to yes to include a chart of data stream values in the report. The default is yes.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to yes to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. Default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to yes to raise an event when the report is successfully generated. Default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_ExchangeConnectivity

This report allows you to make a statistical analysis of the availability of the Exchange Server.

This report uses connectivity data collected by the ExchangeAvail Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Data settings	Use the following parameters to define the statistical calculation applied to data, and which of the data is displayed.
Hours or percentage on chart	Select whether to illustrate availability by hours or by percentage.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value that is, lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top *N***: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom *N***: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. Default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom *N* or %. For example, only the top 10%. Otherwise, the table shows all data. Default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to yes to include a table in the report that lists parameter settings for the report script. Default is yes.

Description	How to Set It
Include table?	Set to yes to include a table of data stream values in the report. Default is yes.
Include chart?	Set to yes to include a chart of data stream values in the report. Default is yes.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to yes to append a timestamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to yes to raise an event when the report is successfully generated. Default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_MessagesByInterval

Use this Knowledge Script to generate a report about new message traffic, including the number of messages sent, queued, received, and filtered, and the total number of new messages during the monitoring interval.

This report uses data collected by the ServerLoad Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers. Each page shows all the data streams collected from a single computer. • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers. For example, each page shows the value of the *NT_CpuResource-All Threads(#)* data stream from each computer. • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to yes to include a table in the report that lists parameter settings for the report script. Default is yes.
Include table?	Set to yes to include a table of data stream values in the report. Default is yes.
Include chart?	Set to yes to include a chart of data stream values in the report. The default is yes.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to yes to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. Default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to yes to raise an event when the report is successfully generated. Default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_MessageSummary

Use this Knowledge Script to generate a summary of total new message traffic during a monitoring interval, including the number of sent, received, and filtered messages.

This report uses data collected by the ServerLoad Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend. The legend is a truncated form of the data stream legend visible in the Operator Console. • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	Use the following parameters to define the statistical calculation applied to data, and which of the data is displayed.
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value that is, lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top *N***: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom *N***: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/ bottom	Enter a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. Default is no.
Show totals on the table?	If set to yes, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column Default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to yes to include a table in the report that lists parameter settings for the report script. Default is yes.
Include table?	Set to yes to include a table of data stream values in the report. Default is yes.
Include chart?	Set to yes to include a chart of data stream values in the report. Default is yes.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click in the Value column, and click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to yes to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. Default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.

Description	How to Set It
Event for report success?	Set to yes to raise an event when the report is successfully generated. Default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_ServerList

Use this script to generate a report listing all the Exchange Servers that are interacting with a BlackBerry Server service. To be included, each Exchange Server must have at least one user on the BlackBerry Enterprise Server. This report shows the Mail Server name, the organizational unit, and the server type. This script uses data collected by the MessagingServerList Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computers	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to yes to include a table in the report that lists parameter settings for the report script. Default is yes.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to yes to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. Default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to yes to raise an event when the report is successfully generated. Default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 35.

Description	How to Set It
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_SRPConnectionUptime

Use this Knowledge Script to generate a report about the percentage of uptime for the Server Routing Protocol (SRP) connection over a specified time period.

This report uses data collected by the SRPConnectionStatus Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers. Each page shows all the data streams collected from a single computer. • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers. For example, each page shows the value of the *NT_CpuResource-All Threads(#)* data stream from each computer. • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to yes to include a table in the report that lists parameter settings for the report script. Default is yes.
Include table?	Set to yes to include a table of data stream values in the report. Default is yes.
Include chart?	Set to yes to include a chart of data stream values in the report. The default is yes.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to yes to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. Default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to yes to raise an event when the report is successfully generated. Default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_SRPConnectivity

Use this Knowledge Script to generate a report about the connectivity (up or down) of the BlackBerry Server SRP connection over a specified period.

This report uses data collected by the SRPConnectionStatus Knowledge Script.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse [...]** button to select the days of the week to include in your report.
Data settings	Use the following parameters to define the statistical calculation applied to data, and which of the data is displayed.
Hours or percentage on chart	Select whether to illustrate availability by hours or by percentage.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value that is, lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top *N***: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom *N***: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. Default is 25.
Truncate top/bottom?	If set to yes, the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. Default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.

Description	How to Set It
Include parameter help card?	Set to yes to include a table in the report that lists parameter settings for the report script. Default is yes.
Include table?	Set to yes to include a table of data stream values in the report. Default is yes.
Include chart?	Set to yes to include a chart of data stream values in the report. Default is yes.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to yes to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. Default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to yes to raise an event when the report is successfully generated. Default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 35.
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_UserByServer

Use this Knowledge Script to generate a report about the number of users on a BlackBerry Server service. Users are listed and sorted by their association with a messaging server.

This report uses data collected by the UserCountByServer Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to yes to include a table in the report that lists parameter settings for the report script. Default is yes.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to yes to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. Default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to yes to raise an event when the report is successfully generated. Default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 35.

Description	How to Set It
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Report_UserListing

Use this Knowledge Script to generate a report about the number of users on a BlackBerry Server service. Users are listed and sorted by their association with a messaging server.

This report uses data collected by the UserList Knowledge Script.

Resource Object

Report Agent > AM Repositories > *AppManager repository*

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to open the time browser. Set a specific or sliding time range for data included in your report.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to yes to include a table in the report that lists parameter settings for the report script. Default is yes.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. Default is no.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired.
Add time stamp to title?	Set to yes to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. Adding a timestamp is useful in order to run consecutive iterations of the same report without overwriting previous output. Default is no.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to yes to raise an event when the report is successfully generated. Default is yes.
Severity level for report success	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 35.

Description	How to Set It
Severity level for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 25.
Severity level for report failure	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

ResponseTime

Use this Knowledge Script to measure the round-trip response time of an email message sent to a BlackBerry handheld and a response received from the handheld. Response time is measured using a pair of script iterations. The first time this Knowledge Script runs, the AppManager agent on the selected computer sends a test email message from the mailbox specified in the "Sender Mailbox" parameter to the handheld by way of a specified Exchange Server that is, the "Sender Mail Server" parameter.

The test message includes an instruction to the handheld to send an automated reply. On the second script iteration, the agent checks for the reply and calculates the response time. The BlackBerry Enterprise Server places a timestamp on the message on its way to the handheld and a timestamp on the reply sent from the handheld. The agent uses these timestamps to calculate the response time.

An event is raised if the response-time threshold is crossed. An event may also indicate that messages failed to be sent or delivered.

Resource Object

BlackBerry Enterprise Server

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise an event if the response time exceeds the threshold. Default is y.
Collect data for round-trip response time?	Set to **y** to collect data for charts and reports. If set to **y**, returns the round-trip response time for the email message. Default is y.
Threshold -- Maximum response time	Enter the maximum response time, in seconds, allowed for the email message to be sent and for a response to be received before an event is raised. Enter a value from 0 to 32000 seconds. Default is 180 seconds.
Sender Mailbox (originates test message)	Enter the name of the mailbox from which the test email message should be sent to the handheld. Default is `netiq-blackberry`.
Sender Mail Server (sends test message to handheld)	Enter the name of the mail server through which the email message should be sent. Default is `mail-server`.
Email address of handheld (receives test message)	Enter the email address of the handheld device that will receive the test message via SMTP and reply to it. Default is `netiq-test-reply@netiq.com`.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 8.

ServerHealth

Use this Knowledge Script to monitor BlackBerry Enterprise Server health. This script monitors the percentage of memory and of CPU time used by instances of the BlackBerry Server service (`BlackBerryServer.exe`). For versions 3.5 and 3.6 of the BlackBerry Enterprise Server, up to 4 instances of this process may be running; their utilization percentages are then totaled. Earlier versions of BlackBerry Enterprise Server do not support multiple instances of `BlackBerryServer.exe`.

If the memory or CPU utilization exceeds either of the thresholds you set, an event is raised.

Resource Object

BlackBerry Enterprise Server

Default Schedule

The default schedule is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if either threshold exceeded?	Set to **y** to raise an event when a threshold is exceeded. Default is y.
Collect data for memory and CPU utilization?	Set to **y** to collect data for charts and reports. If set to **y**, reports the percentage of memory and of CPU time used by the BlackBerry Enterprise Server processes and compares the data collected in the current monitoring interval to that of the previous monitoring interval. Any graphs you create plot the delta rather than the total value. Default is n.
Threshold -- Maximum memory utilization	Enter the maximum percentage of memory that can be used before an event is raised. Enter a value from 0% to 100%. Default is 50%.
Threshold -- Maximum CPU utilization	Enter the maximum CPU utilization (%) allowed by the BlackBerry Enterprise Server processes before an event is raised. Enter values from 0% to 100%. Default is 50%.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the threshold-crossing event. Default is 8.

ServerLoad

Use this Knowledge Script to monitor the number of new messages filtered, sent, received, or queued during an interval. This script also monitors the total number of new messages for the interval.

Note
It is a good idea to set a low threshold so the queue does not grow too large.

If any of the thresholds you set for the number of new, filtered, sent, received, or queued messages is exceeded, an event is raised.

The total of all new messages is measured by calculating at each script iteration the change (delta) between the previous count and the current count of the following:

- Positive change in messages filtered
- Positive change in messages sent
- Positive change in messages received
- Positive or negative change in number of messages in the current queue

Note
The total number of new messages is 0 if there are no new messages. However, the count could also be 0 if the BlackBerry Enterprise administrator resets the Global Redirection Filter statistics counter in the Microsoft Management Console (MMC) to 0.

Resource Object

BlackBerry Enterprise Server

Default Schedule

The default schedule is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if any threshold exceeded?	Set to **y** to raise an event for the number of new messages filtered, sent, received, or queued during an interval. Default is y.
Collect data for new messages filtered, sent, received, or queued?	Set to **y** to collect data for charts and events. If set to **y**, collects number of messages filtered, sent, received, or queued, and total number of new messages during a monitoring interval. Default is n.
Threshold -- Maximum number of messages filtered	Enter the maximum number of messages that can be filtered before an event is raised. Enter a value from 0 to 9999 messages. Default is 50 messages.
Threshold -- Maximum number of messages sent	Enter the maximum number of messages that can be sent before an event is raised. Enter a value from 0 to 9999 messages. Default is 50 messages.

Description	How to Set It
Threshold -- Maximum number of messages received	Enter the maximum number of messages that can be received before an event is raised. Enter a value from 0 to 9999 messages. Default is 50 messages.
Threshold -- Maximum number of messages queued for delivery	Enter the maximum number of messages that can be queued for delivery before an event is raised. Enter a value from 0 to 9999 messages. Default is 50 messages.
Threshold -- Maximum total new messages	Enter the maximum total number of new messages for the monitoring interval. Enter a value from 0 to 9,999 messages. Default is 50 messages.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 8.

ServicesDown

Use this Knowledge Script to monitor the up or down status of BlackBerry Enterprise Server services. You also have the option to restart a service that is down. If any BlackBerry Enterprise Server service is down, or if an attempt to restart fails or succeeds, an event is raised.

You can customize this script to perform the following tasks:

- Restart any service that is down.
- Raise an event if attempt to restart succeeds or fails, or if the "Restart service if down?" parameter is disabled.
- Perform specified actions, such as sending an email to an associated user, when specified events are raised.

You can monitor any or all of the following services:

- BlackBerry Enterprise Server Alert
- BlackBerry Enterprise Server User Admin service
- BlackBerry Server service

Resource Object

BlackBerry Enterprise Server

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Collect data for service status?	Set to **y** to collect data for charts and reports. If set to **y**, returns the following: • 100 -- service is up. • 0 -- service is down. • The percentage of time a service was up. Default is n.
Restart service if down?	Set to **y** to automatically restart any service that is detected down. Default is y.
Event severity for restart failure	Set the event severity level, from 1 to 40, to indicate the importance of the event if the service is down and AppManager cannot restart it. Default is 5.
Event severity for restart success	Set the event severity level, from 1 to 40, to indicate the importance of the event if the service was down and AppManager successfully restarted it. Default is 25.
Event severity when Restart parameter disabled	Set the event severity level, from 1 to 40, to indicate the importance of the event if the service is down and AppManager has not been set to restart it. Default is 18.

Description	How to Set It
Monitor BlackBerry Enterprise Server?	Set to **y** to monitor the BlackBerry Enterprise Server. Default is y.
Monitor BESAlert?	Set to **y** to monitor the `BlackberryAlert` service. Default is y.
Monitor BBUserAdminService?	Set to **y** to monitor the `BBUserAdmin` service. Default is n.
Monitor BlackBerry Mobile Data Server service?	Set to **y** to monitor the BlackBerry Server Mobile Data Server service. This service is only available on BlackBerry Enterprise Server versions 3.5 and later. Default is n.
Check BlackBerry Database Consistency Service?	Set to **y** to monitor the BlackBerry Database Consistency Service. This service is only available on BlackBerry Enterprise Server versions 3.5 and higher. Default is n.
List of services to monitor (comma-separated)	List services to monitor, separated by commas (,). For example: `BBUserAdmin,BlackberryAlert.`

SNMPAlertForward

Use this Knowledge Script to monitor and filter information in the Windows Event Log. If events are found that match the event types you select for monitoring, this script sends an alert in SNMP format.

On the **Actions** tab for this Knowledge Script, Action_SNMPTrap is selected by default.

Resource Object

BlackBerry Enterprise Server

Default Schedule

The default schedule is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if log entries found?	Set to **y** to raise events if Windows Event Log entries are found that match the selected type. Default is y.
Collect data for number and type of event log entries?	Set to **y** to collect data for charts and reports. If set to **y**, returns the number and type of events found in the Windows Event Log that match the event types you enabled. Default is n.
Separate log data from different sources into multiple events?	Set to **y** to separate event entries from the different log files into different data streams. If set to n, all the event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. For example, if you are monitoring both the System and Application logs, set this parameter to **y** to track events in the System log separately from events in the Application log. Default is n.
Filter by log source: System, Security, Application	Specify the event log you want to monitor. You can specify multiple event logs separated by commas. For example, `System,Security,Application`. Default is `Application`.
Filter by event type: Error? Warning? Information? Success Audit? Failure Audit?	Set any or all of the event types to **y** to monitor for this type of event in the Windows Event Log. All defaults are y.
Filter by event source	Enter the appropriate string to monitor events generated by a particular source, such as `SQLExecutive` or `SNMP`. The Knowledge Script looks for matching entries in the **Source** field of each event. You can enter multiple strings separated by commas and include or exclude criteria using a colon (:). If you are only specifying include criteria, the colon is not necessary. Default value is `BlackBerry`.

Description	How to Set It
Filter by event category	Enter the appropriate string to monitor events generated in a particular category, such as Server or Logon. The Knowledge Script looks for matching entries in the **Category** field of each event. You can enter multiple strings separated by commas and include or exclude criteria using a colon (:). If you are only specifying include criteria, the colon is not necessary.
Filter by event ID	Enter an appropriate search string or event ID range such as, 100-2000, to monitor events with particular event IDs. The Knowledge Script looks for matching entries in the **Event** field of each event. You can enter multiple IDs and ranges separated by commas. For example: `1,2, 10-15, 202.` You can also include or exclude criteria using a colon (:). If you are only specifying include criteria, the colon is not necessary.
Filter by event user	Enter an appropriate search string, such as `<domain name>\<user name>`, to monitor for events associated with a particular user. The Knowledge Script looks for matching entries in the **User** field of each event. You can enter multiple strings separated by commas and include or exclude criteria using a colon (:). If you are only specifying include criteria, the colon is not necessary.
Filter by computer	Enter an appropriate search string, such as `netiqjonesr01`,to monitor events associated with a particular computer. The Knowledge Script looks for matching entries in the **Computer** field of each event. You can enter multiple strings separated by commas and include or exclude criteria using a colon (:). If you are only specifying include criteria, the colon is not necessary.
Filter by event description	Enter an appropriate search string, such as "`The SQLSERVERAGENT service terminated unexpectedly`". The Knowledge Script looks for matching entries in the **Description** field of each event. You can enter multiple strings separated by commas and include or exclude criteria using a colon (:). If you are only specifying include criteria, the colon is not necessary.
Maximum number of log entries per event	Specify the maximum number of entries to be recorded into each event detail message. If more entries are found in the log than can be placed in one event message, multiple events are raised to report all log entries. Default is 30 entries per event.
Event severity when matching log entries found	Set the event severity level, from 1 to 40, to indicate the importance of the event when log entries are found that match the criteria. Default is 8. You may want to adjust the severity depending on which log or type of event you are checking for.

SRPConnectionStatus

Use this Knowledge Script to monitor the percentage of uptime during the monitoring interval for the Server Routing Protocol (SRP) connection between the BlackBerry Server and the Research in Motion (RIM) infrastructure.

SRP makes a TCP/IP connection to the wireless network to transmit email messages to and from your wireless ISP. SRP is built on top of a TCP session between Port 3101 of the BlackBerry Enterprise Server and the IP address `srp.blackberry.net` or `srp.na.blackberry.net.`

If the percentage of uptime fails to meet the threshold, an event is raised.

Note

This script is unable to provide SRP connection status information more frequently than 1 sample per minute. Thus, if you change the default interval to less than Every 1 minute, such as, Every 20 seconds, the script only reports one data point every 20 seconds, but the data point represents the SRP connection status for the past minute.

Resource Object

BlackBerry Enterprise Server SRP connection

Default Schedule

The default schedule is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if threshold not met?	Set to **y** to raise an event if the BlackBerry Server SRP connection is down or if WinSock error messages appear in the debug log. Default is y.
Collect data for SRP connection uptime?	Set to **y** to collect data for charts and events about the BlackBerry Server SRP connection. If set to **y**, this script returns data about the first ping test that was run and the associated status such as, success or failure, as well as the date and time of the ping test. Default is n.
Threshold -- Minimum SRP connection uptime	Enter the lowest percentage of SRP connection uptime allowed before an event is raised. Enter a value from 0% to 100%. Default is 60%.
Event severity when threshold not met	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

SRPTest

Use this Knowledge Script to perform a Ping test of the BlackBerry Server SRP connection and display the result. An event is raised when the BlackBerry Server SRP connection returns a non-zero exit code meaning that the connection could not be reached. The script can also raise an event if the ping test is successful.

For more information about the SRP connection, see the SRPConnectionStatus Knowledge Script.

Note
This Knowledge Script requires the BBSRPTest utility to run.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if test or job fails?	If set to n, this Knowledge Script raises an event when the Ping test to the BlackBerry Server SRP connection returns a non-zero exit code. If set to **y**, the script raises an event when the ping is successful. An event is always raised on script failure, if the ping test cannot be run. Default is y.
Collect data for SRP connection status?	Set to **y** to collect data for charts and reports. If set to **y**, returns the status of the BlackBerry Server SRP connection. Default is n.
BBSRPTest utility timeout	Set a timeout value from 1 to 120 seconds. The Knowledge Script keeps trying to locate the BBSRPTest utility, which is required to run the Ping test, until the timeout expires. Default is 20 seconds.
Path and filename for BBSRPTest utility	Enter the path and filename for the BlackBerry utility required to run the Ping test. Leave blank to use the BlackBerry default path.
Event severity: Ping succeeded	Set the event severity level, from 1 to 40, to indicate the importance of the event when the Ping test was successful. Default is 25.
Event severity: Ping returned non-zero exit code	Set the event severity level, from 1 to 40, to indicate the importance of the event when the Ping test returned a non-zero exit code. Default is 8.
Event severity: SRPTest command failed	Set the event severity level, from 1 to 40, to indicate the importance of the event when the script fails. Default is 40.

UserCountByServer

Use this Knowledge Script to report the number of users on a BlackBerry Server. Users are listed and sorted by their association with a messaging (Exchange) server. An event is raised if the total user count exceeds the threshold.

Note
This Knowledge Script requires the BBUserAdminClient executable to run.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every week**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if script succeeds?	Set to **y** to raise an event if the list of users is successfully generated. Default is n.
Raise event if threshold exceeded?	Set to **y** to raise an event if the threshold for number of users is exceeded. Default is y.
Collect data for users and servers?	Set to **y** to collect data for charts and reports. If set to **y**, returns a list of users of a BlackBerry Enterprise Server, sorted by their associated Exchange Server. Default is y.
Threshold -- Maximum number of users	Enter the maximum total number of users allowed before an event is raised. Enter a value from 0 to 9000. Default is 300.
Path and filename for `BBUserAdminClient` executable	Enter the path and filename for the BlackBerry executable required to run the job. Leave blank to use the BlackBerry default path.
`BBUserAdminClient` executable timeout	Set a timeout value to determine how long the script attempts to reach the `BBUserAdminClient` executable. Enter a value from 1 to 120 seconds. Default is 10 seconds.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 25.

UserList

Use this Knowledge Script to report all the users on a BlackBerry Server, and the total number of users on the BlackBerry Enterprise Server. By default, this script lists all the users and sorts them based on the Exchange Server they are associated with. You can also sort users alphabetically.

Note
This Knowledge Script requires the BBUserAdminClient executable to run.

Resource Object

BlackBerry Server

Default Schedule

The default schedule is **Every week**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event if script succeeds?	Set to **y** to raise an event when the job completes successfully. Default is n.
Raise event if threshold exceeded?	Set to **y** to raises an event when the threshold is exceeded. Default is y.
Collect data for number of users?	Collects data about the number of users on the BlackBerry Server. Default is y.
Threshold -- Maximum total number of users	Enter the maximum number of users of the BlackBerry Enterprise Server allowed before an event is raised. Enter a value from 0 to 900000. Default is 1500.
Threshold -- Maximum users per BlackBerry Server	Enter the maximum number of users of a BlackBerry Server allowed before an event is raised. Enter a value from 0 to 900000. Default is 300.
Sort by Exchange Server?	Set to **y** to sort the list of users by each user's Exchange Server. Set to n to sort the list of users alphabetically. Default is y.
Path and filename for `BBUserAdminClient` executable	Enter the path and filename for the BlackBerry executable required to run the job. Leave blank to use the BlackBerry default path.
`BBUserAdminClient` executable timeout	Set a timeout value to determine how long the script attempts to reach the `BBUserAdminClient` executable, from 1 to 120 seconds. The default is 10 seconds.
Event severity when either threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the threshold-crossing event. Default is 25.

Chapter 16
CallData Knowledge Scripts

AppManager for Call Data Analysis provides the following Knowledge Scripts. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AddDataSource_CiscoCallMgr	Adds a Unified Communications Manager version 4.x Data Source and its associated Data Mart.
AddDataSource_CiscoCM	Adds a Unified Communications Manager Data Source (versions 5.x - 7.x) and its associated Data Mart.
AddDataSource_H323RADIUS	Adds an H.323 RADIUS Data Source and its associated Data Mart.
CancelDataCollection	Cancels the current execution of data collection.
CCME_GetConfig	Retrieves configuration information from one or more Communications Manager Express devices.
ChangeReportingState	Changes the state of a Data Mart to be included in or excluded from reporting.
ChangeSchedule	Changes, deactivates, or reactivates the data collection schedule associated with a Data Source.
ConfigureCallTypes	Configures the rules by which the Call Data Analysis module classifies the types of calls each CDR contains.
DataCollectionStatus	Checks the status of the last data collection job performed against a Data Source.
ExecuteDataCollection	Performs on-demand data collection regardless of the collection schedule.
RemoveDataSource	Removes a Data Source and its associated Data Mart.
Report_CallAuthorization	Summarizes the number and duration of calls that used a Forced Authorization Code or a Client Matter Code.
Report_CallCompletionRate	Summarizes the completion rate of calls recorded with the selected Data Source. The call completion rate takes into account failed calls and abandoned calls.
Report_CallDetail_CiscoCallMgr	Summarizes details for calls that match criteria you specify for a selected Communications Manager. Call details can include time, calling number, and called number.
Report_CallDetail_H323Gateway	Summarizes details for calls that match criteria you specify for a selected gateway. Call details can include time, calling number, and called number.

Knowledge Script	What It Does
Report_CallFailureCauses	Analyzes the failure causes for calls that match criteria you specify.
Report_CallJitter	Categorizes calls as having good, acceptable, or poor jitter based on thresholds you specify.
Report_CallJitterLoss	Categorizes jitter loss percentages as good, acceptable, or poor based on thresholds you specify.
Report_CallMOS	Categorizes calls as having good, acceptable, or poor MOS or R-value based on thresholds you specify.
Report_CallPacketLoss	Categorizes calls as having good, acceptable, or poor packet loss based on thresholds you specify.
Report_CallQualityByPhone	Identifies the directory numbers that are experiencing problems with call quality, such as jitter and packet loss.
Report_CallSuccessRate	Summarizes the success rate of calls recorded with the selected Data Source. A successful call is determined by the call's disconnect cause code.
Report_CallTraffic	Summarizes call traffic based on call type.
Report_CallVolume	Summarizes the number and duration of calls recorded with the selected Data Source.
Report_CCME_StatsByEPhone	Summarizes call statistics per Communications Manager Express ephone.
Report_CCME_Summary	Summarizes call statistics per Communications Manager Express gateway.
Report_FrequentlyCalledNumbers	Summarizes phone numbers called frequently during a specified time range.
Report_GatewayDialPeers	Summarizes call statistics for POTS and VoIP dial peers for the gateways included in the report.
Report_TrunkGroupByHour	Summarizes the trunk group or gateway volume by hour for the selected Communications Manager cluster or H.323 RADIUS Data Source.
Report_UnusedPhones	Creates a list of unused phones based on phones registered to the selected Data Source.
UpdateSecurity	Updates the user IDs and passwords associated with a Data Source.

AddDataSource_CiscoCallMgr

Use this Knowledge Script to add a Unified Communications Manager version 4.x Data Source. With this script, you configure the Data Source and its collection schedule, the associated Data Mart, and access to the Data Warehouse. This script raises an event if a Data Source is added successfully, if the Data Mart server is inaccessible, if warnings are raised during an attempt to add a Data Source, and if a Data Source is not added.

This script creates the Data Mart, which is the container for all configuration and CDR information it gathers from the Data Source according to a schedule you determine.

AppManager needs to wait for the Communications Manager Publisher to receive the CDRs for completed calls from the Subscribers and push them into the CDR database. This buffer time is one hour. Therefore, after a call completes, you need to wait a minimum of one hour before the call is available for collection.

Note
After you run AddDataSource_CiscoCallMgr, press **[F5]** to refresh the Operator Console and display the other Knowledge Scripts available in the AppManager for Call Data Analysis module.

Prerequisite

Set Windows authentication permissions on the Communications Manager server and the Data Mart computer.

Resource Object

Call Data server

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Configure Data Source	
Server name	Provide the computer name of the Communications Manager Publisher that will be the source of the CDR data.
SQL username	Provide the SQL username required to access the Communications Manager Publisher. Leave this field blank to use Windows authentication.
SQL password	Specify the SQL password associated with the username you entered in the previous parameter.
Configure Data Source Schedule	
Data source schedule type	Select the frequency with which you want the Data Mart to collect data from the Data Source: **Daily** or **Hourly**. The default is Daily.

Parameter	How to Set It
Daily start time - Run daily at	If you selected **Daily** above, select the time of day at which you want data collected. Select from a list of hours based on a 24-hour clock. For instance, select 0100 for 1:00 AM. or select 1300 for 1:00 PM. The default is 0400. **Notes** • No matter what start time you select, AppManager needs to wait for the Communications Publisher to receive the CDRs for completed calls from the Subscribers and populate them into the CDR database. This buffer time is 1 hour. Therefore, after a call completes, you will need to wait a minimum of 1 hour before the call is available for collection. For instance, if you select 0400, data is collected up through 0300 to ensure no data is missed if the Communications Manager database is behind in writing its CDRs. • If you have multiple Data Sources, you may want to stagger your data collection times in order to balance the load on the Data Warehouse.
Hourly time interval - Run every n hours	If you selected **Hourly** above, select the interval at which you want data collected, such as every 2 hours or every 8 hours. The default is 12 hours. **Notes** • No matter what start time you select, AppManager needs to wait for the Communications Manager Publisher to receive the CDRs for completed calls from the Subscribers and populate them into the CDR database. This buffer time is 1 hour. Therefore, after a call completes, you will need to wait a minimum of 1 hour before the call is available for collection. For instance, perhaps you select every 2 hours, and the script collects data at 2 PM, 4 PM, and 6 PM. At 2 PM, data is gathered from 11 AM to 1 PM; at 4 PM, data is gathered from 1 PM to 3 PM; and at 6 PM, data is gathered from 3 PM to 5 PM to ensure no data is missed if the Communications Manager database is behind in writing its CDRs. • If you have multiple Data Sources, you may want to stagger your data collection times in order to balance the load on the Data Warehouse.
Data Collection	
Initially load n days of data	Specify the number of days' worth of accumulated data you want the Data Mart to collect during its first instance of data collection. The default is 7 days' worth of data.
Start data collection immediately?	Select **Yes** if you want the Data Mart to collect data immediately, rather than waiting for the first scheduled collection. The default is unselected. The first time the data collection job runs, it collects data for the past *n* days. When deciding whether to start data collection immediately, consider the impact the first, possibly large, data collection might have on your Communications Manager Publisher computer. You should perform the initial collection at an off-peak time.
Start SQL Server Agent if it is stopped?	Select **Yes** to start SQL Server Agent. SQL Server Agent must be running in order for data collection tasks to be performed. The default is unselected.
Keep data for n months	Specify the number of months' worth of collected data you want to keep in the database on the Data Mart. The data for the current month is always kept in the database. Therefore, if you choose to keep one month's worth of data, and it is December, the database will retain the data for December and November.
Configure Data Mart	
Server name	Specify the name of the server on which the Data Mart database will be created. If you leave this field blank, the Data Mart will be created on the same server as the Data Warehouse.

Parameter	How to Set It
SQL username	Specify the SQL username required to access the Data Mart server. Leave this field blank to use Windows authentication.
SQL password	Specify the SQL password associated with the username you entered in the previous parameter.
Data Warehouse Access	
SQL username	Specify the username required to access the SQL Server running on the Data Warehouse FROM the local NetIQ agent (`netiqmc` service) AND the SQL Server agent service running on the Data Mart computer. Leave this field blank to use Windows authentication. **Note** If you leave this field blank, and the Data Mart is not located on the Data Warehouse computer, verify the `SQLSERVERAGENT` service on the Data Mart computer is running as a user that has access to the Data Warehouse database.
SQL password	Specify the SQL password associated with the username you entered in the previous parameter.
Event Notification	
Raise event if job succeeds?	Select **Yes** to raise an informational event when the AddDataSource job is successful. The default is Yes.
Event severity when job succeeds	Set the severity level, from 1 to 40, to reflect the importance of an event in which the AddDataSource job is successful. The default is 25.
Event severity when data mart server inaccessible	Set the severity level, from 1 to 40, to reflect the importance of an event in which the Data Mart server is inaccessible. The default is 10.
Event severity for warnings	Set the severity level, from 1 to 40, to reflect the importance of warnings raised during an attempt to add a Data Source. The default is 20.
Event severity when job fails	Set the severity level, from 1 to 40, to reflect the importance of an event in which the AddDataSource job fails. The default is 5.

AddDataSource_CiscoCM

Use this Knowledge Script to add a Cisco Unified Communications Manager (versions 5.x -7.x) Data Source. With this script, you configure the Data Source and its collection schedule, the associated Data Mart, and access to the Data Warehouse. This script raises an event if a Data Source is added successfully, if the Data Mart server is inaccessible, if warnings are raised during an attempt to add a Data Source, and if a Data Source is not added.

This script creates the Data Mart, which is the container for all configuration and CDR information it gathers from the Data Source according to a schedule you determine.

AppManager needs to wait for the Communications Manager primary server to push the CDRs to the Cisco CM managed object computer, and then for the CiscoCM_CDR_RetrieveCallRecords Knowledge Script to insert them into the Cisco CM supplemental database. This buffer time is one hour. Therefore, after a call completes, you need to wait a minimum of one hour before the call's CDR is available for collection.

Note
After you run AddDataSource_CiscoCM, press **[F5]** to refresh the Operator Console and display the other Knowledge Scripts available in the Call Data Analysis module.

Prerequisites

- Using the AppManager for Cisco Unified Communications Manager module, run the CiscoCM_SetupSupplementalDB Knowledge Script to create the Cisco CM supplemental database.
- Using the AppManager for Cisco Unified Communications Manager module, run the CiscoCM_CDR_RetrieveConfigData and CiscoCM_CDR_RetrieveCallRecords Knowledge Scripts to populate the supplemental database with configuration and call data from Communications Manager. After the supplemental database is populated, you can report on the data using the wide variety of Report Knowledge Scripts provided by AppManager for Call Data Analysis.

Resource Object

Call Data server

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Configure Data Source	
Primary Cisco Unified CallManager server	Specify the computer name of the Communications Manager primary server that is the source of the CDA data stored in the Cisco CM supplemental database.

Parameter	How to Set It
Supplemental database SQL Server	Specify the computer name of the SQL Server computer that houses the Cisco CM supplemental database. Leave this parameter blank to create a supplemental database on the Data Warehouse computer.
SQL username	Specify the SQL username required to access the Cisco CM supplemental database. Leave this field blank to use Windows authentication.
SQL password	Specify the SQL password associated with the username you entered in the previous parameter.
Configure Data Source Schedule	
Data source schedule type	Select the frequency with which you want the Data Mart to collect data from the Data Source: **Daily** or **Hourly**. The default is Daily.
Daily start time - Run daily at	If you selected **Daily** above, select the time of day at which you want data collected. Select from a list of hours based on the 24-hour time system. For instance, select 0100 for 1:00 AM or select 1300 for 1:00 PM. The default is 0400. **Notes** • No matter what start time you select, AppManager needs to wait for the Communications Manager primary server to push the CDRs to the Cisco CM managed object computer, and then for the CDR_RetrieveCallRecords script to insert them into the Cisco CM supplemental database. This buffer time is one hour. Therefore, after a call completes, you will need to wait a minimum of one hour before the CDR is available for collection. For instance, if you select 0400, data is collected up through 0300 to ensure no data is missed if the primary server is behind in writing its CDRs. • If you have multiple Data Sources, you may want to stagger your data collection times in order to balance the load on the Data Warehouse.
Hourly time interval - Run every n hours	If you selected **Hourly** above, select the interval at which you want data collected, such as every 2 hours or every 8 hours. The default is 12 hours. **Notes** • No matter what start time you select, AppManager needs to wait for the Communications Manager primary server to push the CDRs to the Cisco CM managed object computer, and then for the CDR_RetrieveCallRecords script to insert them into the Cisco CM supplemental database. This buffer time is one hour. Therefore, after a call completes, you will need to wait a minimum of one hour before the CDR is available for collection. For instance, if you select 0400, data is collected up through 0300 to ensure no data is missed if the primary server is behind in writing its CDRs. • If you have multiple Data Sources, you may want to stagger your data collection times in order to balance the load on the Data Warehouse.
Data Collection	
Initially load n days of data	Specify the number of days' worth of accumulated data you want the Data Mart to collect during its first instance of data collection. The default is 7 days' worth of data.
Start data collection immediately?	Select **Yes** if you want the Data Mart to collect data immediately, rather than waiting for the first scheduled collection. The default is unselected. The first time the data collection job runs, it collects data for the past *n* days. When deciding whether to start data collection immediately, consider the impact the first, possibly large, data collection might have on the computer that houses the Cisco CM supplemental database. You should perform the initial collection at an off-peak time.

Parameter	How to Set It
Start SQL Server Agent if it is stopped?	Select **Yes** to start SQL Server Agent. SQL Server Agent must be running in order for data collection tasks to be performed. The default is unselected.
Keep data for n months	Specify the number of months' worth of collected data you want to keep in the database on the Data Mart. The data for the current month is always kept in the database. Therefore, if you choose to keep 1 month's worth of data, and it is December, the database will retain the data for December and November.
Configure Data Mart	
Server name	Specify the name of the server on which the Data Mart database will be created. If you leave this field blank, the Data Mart will be created on the same server as the Data Warehouse.
SQL username	Specify the SQL username required to access the Data Mart server. Leave this field blank to use Windows authentication.
SQL password	Specify the SQL password associated with the username you entered in the previous parameter.
Data Warehouse Access	
SQL username	Specify the username required to access the SQL Server running on the Data Warehouse FROM the local NetIQ agent (`netiqmc` service) AND the SQL Server agent service running on the Data Mart computer. Leave this field blank to use Windows authentication. **Note** If you leave this field blank, and the Data Mart is not located on the Data Warehouse computer, verify the `SQLSERVERAGENT` service on the Data Mart computer is running as a user that has access to the Data Warehouse database.
SQL password	Specify the SQL password associated with the username you entered in the previous parameter.
Event Notification	
Raise event if job succeeds?	Select **Yes** to raise an informational event when the AddDataSource job is successful. The default is Yes.
Event severity when job succeeds	Set the severity level, from 1 to 40, to reflect the importance of an event in which the AddDataSource job is successful. The default is 25.
Event severity when data mart server inaccessible	Set the severity level, from 1 to 40, to reflect the importance of an event in which the Data Mart server is inaccessible. The default is 10.
Event severity for warnings	Set the severity level, from 1 to 40, to reflect the importance of warnings raised during an attempt to add a Data Source. The default is 20.
Event severity when job fails	Set the severity level, from 1 to 40, to reflect the importance of an event in which the AddDataSource job fails. The default is 5.

AddDataSource_H323RADIUS

Use this Knowledge Script to add an H.323 RADIUS Data Source for call detail records from Cisco H.323 gateways and Cisco Communications Manager Express routers. With this script, you will configure the Data Source and its collection schedule, the associated Data Mart, and access to the Data Warehouse.

This script creates the Data Mart, which is the container for all configuration and CDR information it gathers from the Data Source according to a schedule you determine.

The H.323 RADIUS Data Source is the log (flat) files written by the IAS/RADIUS server when it receives call detail records generated by Cisco H.323 gateways and Communications Manager Express routers.

Cisco Communications Manager Express views the IP phones connected to it as virtual voice ports (EFXS) and generates telephony call legs to and from these phones. Therefore, call quality information is not available for a call from Communications Manager Express phones for which the call remains on Communications Manager Express or goes directly to the PSTN.

This script raises an event if a Data Source is added successfully, if the Data Mart server is inaccessible, if warnings are raised during an attempt to add a Data Source, and if a Data Source is not added.

You can re-run this Knowledge Script to change parameter settings, such as log file archiving. If you do so, you need to complete all parameters, not just those you are changing.

Note
After you run AddDataSource_H323RADIUS, press **[F5]** to refresh the Operator Console and display the other Knowledge Scripts available in the Call Data Analysis module.

Changing RADIUS Log Folder or Archive Settings

When you add a Data Source, you specify whether to archive RADIUS logs after processing. In addition, you indicate the location of the RADIUS logs and the location of the archive folder.

To change any of these settings for a Data Source you already added, rerun AddDataSource_H323RADIUS and complete all parameters, including those for which the setting is not changing:

- *Folder containing IAS RADIUS logs*. Use this parameter to specify the location on the Data Mart of the folder that houses the IAS RADIUS logs. This location is the one you set up when you configured IAS.
- *Archive RADIUS logs after processing?* Set this parameter to **Yes** if you want to archive the RADIUS logs after their data has been processed. If you set this parameter to **Yes**, you must use the *Archive folder* parameter to specify the location of the archive folder.
- *Archive folder*. Use this parameter to specify the location on the Data Mart of the folder in which you want to archive the processed RADIUS logs.

Note
If you rerun AddDataSource_H323RADIUS, all parameters are updated, not only the three discussed above. Therefore, if you originally added your Data Source with any non-default parameter values, ensure you set those parameters correctly when you run the script to change archive or log information.

Reviewing Call Quality Metrics for Gateways and Routers

Cisco H.323 gateways provide call quality information for the VoIP legs of a call. Using this information, AppManager calculates additional quality metrics.

MOS

The Mean Opinion Score) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. The MOS is calculated based on measured items plus jitter buffer size.

R-value

Can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor).

Jitter loss

Calculated from the number of received and discarded packets. Discarded packets are those that arrive too early or too late to be stored in the jitter buffer.

Packet loss

Calculated from the number of received and lost packets.

Delay

One-way delay approximated by dividing the round-trip delay value (from the RADIUS record) by two.

Voice quality

The Cisco IOS software (which is installed on the router on which the H.323 gateway resides) measures call quality based on ITU G.113, which defines the term Calculated Planning Impairment Factor (ICPIF), a calculation based on network delay and packet loss. ICPIF yields a single value that can be used to gauge network impairment. ITU G.113 provides the following interpretations of specific ICPIF values:

- 5 - Very good
- 10 - Good
- 20 - Adequate
- 30 - Limiting case
- 45 - Exceptional limiting case
- 55 - Customers likely to react strongly

Note
Use the Report_CallDetail_H323Gateway script to see the ICPIF values for individual calls.

Resource Object

Call Data server

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Configure Data Source	
Folder containing IAS RADIUS logs	Specify the location on the Data Mart of the folder that houses the IAS RADIUS logs. This location is the one you set up when you configured IAS.
Configure Data Source Schedule	
Data source schedule type	Select the frequency with which you want the Data Mart to collect data from the Data Source: **Daily** or **Hourly**. The default is Daily.
Daily start time - Run daily at	If you selected **Daily** above, select the time of day at which you want data collected. Select from a list of hours based on a 24-hour clock. For instance, select 0100 for 1:00 A.M. or select 1300 for 1:00 P.M. The default is 0400. **Note** If you have multiple Data Sources, you may want to stagger your data collection times in order to balance the load on the Data Warehouse.
Hourly time interval - Run every n hours	If you selected **Hourly** above, select the interval at which you want data collected, such as every 2 hours or every 8 hours. The default is 12 hours. **Note** If you have multiple Data Sources, you may want to stagger your data collection times in order to balance the load on the Data Warehouse.
Data Collection	
Archive RADIUS logs after processing?	Select **Yes** to archive the RADIUS logs after their data has been processed. The default is unselected. If you set this parameter to Yes, specify the location of the archive folder in the *Archive folder* parameter.
Archive folder	Specify the location on the Data Mart of the folder in which you want to archive the processed RADIUS logs.
Start data collection job immediately?	Select **Yes** if you want the Data Mart to collect data immediately, rather than waiting for the first scheduled collection. The default is unselected.
Start SQL Server Agent if it is stopped?	Select **Yes** to start SQL Server Agent. SQL Server Agent must be running in order for data collection tasks to be performed. The default is unselected.
Keep data for n months	Specify the number of months' worth of collected data you want to keep in the database on the Data Mart. The data for the current month is always kept in the database. Therefore, if you choose to keep 1 month's worth of data, and it is December, the database will retain the data for December and November.
Configure Data Mart	
Server name	Specify the name of the server on which the Data Mart database will be created. If you leave this field blank, the Data Mart will be created on the same server as the Data Warehouse.
SQL username	Specify the SQL username required to access the Data Mart server. Leave this field blank to use Windows authentication.
SQL password	Specify the SQL password associated with the username you entered in the previous parameter.
Data Warehouse Access	

Parameter	How to Set It
SQL username	Specify the username required to access the SQL Server running on the Data Warehouse FROM the local NetIQ agent (`netiqmc` service) AND the SQL Server agent service running on the Data Mart computer. Leave this field blank to use Windows authentication. **Note** If you leave this field blank, and the Data Mart is not located on the Data Warehouse computer, verify the `SQLSERVERAGENT` service on the Data Mart computer is running as a user that has access to the Data Warehouse database.
SQL password	Specify the SQL password associated with the username you entered in the previous parameter.
Event Notification	
Raise event if job succeeds?	Select **Yes** to raise an informational event when the AddDataSource job is successful. The default is Yes.
Event severity when job succeeds	Set the severity level, from 1 to 40, to reflect the importance of an event in which the AddDataSource job is successful. The default is 25.
Event severity when data mart server inaccessible	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the Data Mart server is inaccessible. The default is 10.
Event severity for warnings	Set the event severity level, from 1 to 40, to reflect the importance of warnings raised during an attempt to add a Data Source. The default is 20.
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the AddDataSource job fails. The default is 5.

CancelDataCollection

Use this Knowledge Script to stop any data collection currently being performed. If data is not currently being collected, this script takes no action. Running this script does not affect the data collection schedule.

This script raises an event if data cancellation succeeds or fails, and if data is not being collected.

Resource Objects

Call Data CallManager object

Call Data H.323 RADIUS object

Call Data CiscoCM object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity when cancellation succeeds	Set the severity level, from 1 to 40, to reflect the importance of an event in which cancellation succeeds. The default is 25.
Event severity when no data collection to cancel	Set the severity level, from 1 to 40, to reflect the importance of a situation in which there is no data collection to cancel. The default is 25.
Event severity when cancellation fails	Set the severity level, from 1 to 40, to reflect the importance of an event in which cancellation fails. The default is 5.

CCME_GetConfig

Use this Knowledge Script to retrieve configuration data from one or more Communications Manager Express devices and deposit that data into SQL tables located in the Data Mart. By default, this script retrieves configuration data for all Communications Manager Express devices that have sent RADIUS records to the Data Source and have EFXS (virtual voice) ports through which ephones are connected. However, you can choose to limit the devices by using the "Include" and "Exclude" parameters.

This script raises an event if configuration data is retrieved and deposited successfully, if no Communications Manager Express devices are found, if the retrieve and/or deposit processes fail for any Communications Manager Express device, or if the entire GetConfig job fails for any reason.

The collected configuration data helps AppManager associate the virtual voice port from the RADIUS records with the IP address and device name of the associated Communications Manager Express phone. The data is also required by the Report_CCME_StatsByEPhone and Report_UnusedPhones Knowledge Scripts.

Prerequisites

- Run AddDataSource_H323RADIUS.
- Configure your AXL passwords in AppManager Security Manager. AVVID XML Layer (AXL), a Cisco application programming interface (API), enables Communications Manager Express to access the Communications Manager Express HTTP server.

  If your AXL password information is the same for all Communications Manager Express devices, complete the following procedure once. If your AXL password information is different for different devices, complete the following procedure once for each different password.

  On the Custom tab in AppManager Security Manager, complete the following fields:

Field	Description
Label	`CiscoCME`
Sub-label	• For a single Communications Manager Express device, type the name of the device. • For all Communications Manager Express devices, type `default`. **Note** If you type a single device name, ensure the name is an exact match to the gateway name (`h323-gw-id`) or the `NAS-IP-Address` from the RADIUS records. If you are unsure of the gateway name or NAS IP address, run Discovery_CallDataAnalysis after IAS logs have been processed. The name of the gateway will appear in the TreeView pane under the H.323 Data Source object. To see the NAS IP address, click on the gateway name, and then click the **Details** tab.
Value 1	Type the AXL password you configured using the "og password" IOS command on the router. If you did not configure an AXL password, type the "Router privilege mode" password.
Extended application support	Enable to encrypt the AXL password. Do not leave this checkbox unselected.

Resource Object

Call Data H.323 RADIUS object

Default Schedule

By default, this script runs once every day.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Include only these CallManager Express devices	Specify which Communications Manager Express devices (gateways) to poll for configuration data. Use this parameter to limit the number of "learned" devices that are polled or to poll devices that are not yet "learned." A learned device is one that has already sent RADIUS records to the Data Source. If you specify one or more unlearned devices, you must specify the gateway name that matches the name returned in the `h323_gw_id` field of the RADIUS record. Leave this parameter blank to poll all learned Communications Manager Express devices for configuration data. Separate the names of multiple devices with a comma and no space.
Exclude these CallManager Express devices	Specify which Communications Manager Express devices (gateways) to exclude from polling. Separate the names of multiple devices with a comma and no space. Leave this parameter blank to exclude no devices.
Event Notification	
Raise event if retrieve/deposit process succeeds?	Select **Yes** to raise an event if the configuration data is retrieved and deposited (into the Data Mart SQL tables) successfully. The default is Yes.
Event severity when retrieve/deposit process succeeds	Set the severity level, from 1 to 40, to reflect the importance of an event in which configuration data is retrieved and deposited successfully. The default is 25.
Raise event if no CallManager Express devices found?	Select **Yes** to raise an event if AppManager cannot find any Communications Manager Express devices to poll for configuration data. The default is Yes.
Event severity when no CallManager Express devices found	Set the severity level, from 1 to 40, to reflect the importance of an event in which AppManager can find no Communications Manager Express devices to poll. The default is 15.
Event severity when retrieve/deposit process fails	Set the severity level, from 1 to 40, to reflect the importance of an event in which any part of the retrieve and deposit process fails for any individual Communications Manager Express device. This event is raised if the retrieve/deposit process fails for one or more Communications Manager Express devices, but succeeds for others. The default is 10.
Event severity when job fails	Set the severity level, from 1 to 40, to reflect the importance of an event in which the GetConfig Knowledge Script job fails.

ChangeReportingState

Call Data Analysis reports make use of SQL views that include all Data Marts associated with your Data Sources. The Call Data Analysis reports fail if even one of the Data Marts in a SQL view cannot be accessed from the Data Warehouse.

If you know a particular Data Mart cannot be accessed for some reason (such as being down for maintenance), use this Knowledge Script to exclude that Data Mart from reporting. Then, when the Data Mart is ready, use this Knowledge Script to change its reporting status so it is once again included in reporting.

Note
Highlight the Data Source object in the TreeView of the Operator Console to see the reporting state displayed on the **Details** tab. After changing the reporting state, you may need to click on a different object and then click back on the Data Source object to verify the change in the reporting state.

Resource Objects

Call Data CallManager object

Call Data H.323 RADIUS object

Call Data CiscoCM object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Change Reporting State	
Select the reporting state for the Data Mart	Use this parameter to change whether a Data Mart is included in reporting. Select **Include** to include the Data Mart associated with the Data Source on which you dropped this script. Select **Exclude** to exclude the Data Mart associated with the Data Source on which you ran this script.
Event Notification	
Event severity when reporting state change succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a change in the reporting state succeeds. The default is 25.
Event severity when reporting state change fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a change in the reporting state fails, most likely as the result of a SQL failure. The default is 5.

ChangeSchedule

Use this Knowledge Script to change, deactivate, or reactivate the data collection schedule associated with a Data Source. This script raises an event when a schedule change succeeds or fails, or when a schedule cannot be changed.

To change other data collection settings, such as how many days' worth of data to load, or how many months' worth of data to keep, run the appropriate AddDataSource Knowledge Script. You can run an AddDataSource Knowledge Script even after you added the Data Source.

Resource Objects

Call Data CallManager object

Call Data H.323 RADIUS object

Call Data CiscoCM object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Manage Schedule	
Select Schedule Action	Select the action you want this script to perform: • **Change Schedule**. This default selection allows you to change the schedule type, the collection start time, or the hourly collection interval. If you select Change Schedule, you must set one or more of the parameters in the **Change Schedule Parameters** folder. • **Deactivate Schedule**. Deactivates the data collection schedule. Data collection will not resume until you run this script again and select **Reactivate Schedule**. • **Reactivate Schedule**. Reactivates the data collection schedule and collects data at the next scheduled instance. The Data Mart will collect all data that has accrued since the last collection instance.
Change Schedule Parameters	
Data source schedule type	Select the frequency with which you want the Data Mart to collect data from the Data Source: **Daily** or **Hourly**. The default is Daily.
Daily start time - Run daily at	If you selected **Daily** above (or when you added the Data Source), select the time of day at which you want data collected. Select from a list of hours based on a 24-hour clock. For instance, select 0100 for 1:00 AM or select 1300 for 1:00 PM. The default is 0400.
Hourly time interval - Run every n hours	If you selected **Hourly** above (or when you added the daily source), select the interval at which you want data collected, such as every 2 hours or every 8 hours. The default is 12 hours.
Event Notification	

Parameter	How to Set It
Event severity when schedule change succeeds	Set the severity level, from 1 to 40, to reflect the importance of an event in which the schedule change succeeds. The default is 25.
Event severity when schedule change fails	Set the severity level, from 1 to 40, to reflect the importance of an event in which the schedule change fails. The default is 5.
Event severity when schedule cannot be changed	Set the severity level, from 1 to 40, to reflect the importance of a situation in which the changes you have selected already exist in the schedule. The default is 25.

ConfigureCallTypes

Use this Knowledge Script to configure the rules by which the Call Data Analysis module classifies the types of calls each CDR contains, such as configuring gateway rules that identify certain calls going through the gateway as local rather than long distance.

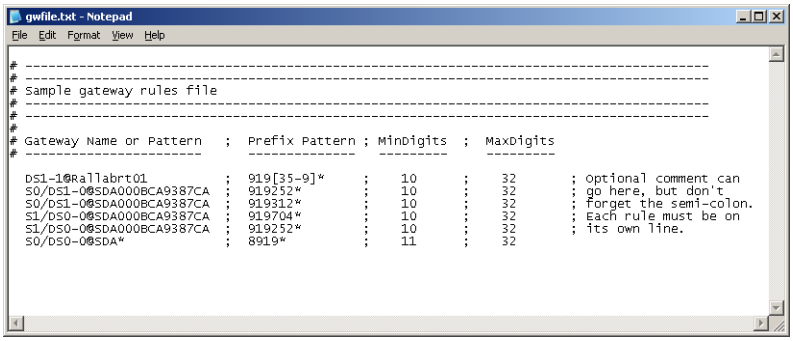
You specify the name of the gateway and the prefixes that indicate a call is local. The prefix is not limited to an area code, which helps in situations in which numbers within the same area code are treated differently. For example, if 919-767-0295 is a local call, but 919-252-7463 is long distance, specify 9197* or 919767* as the prefix pattern.

If all calls within an area code are to be classified as local, specify an "*" as the gateway pattern and specify 919* as the prefix pattern.

Because you may need to specify many gateways or gateway devices, you can create a file that contains a list of all gateways and devices. If you create a list, you do not have to specify each gateway and device separately in the *Gateway names or patterns* parameter. You can use the *Full path to gateway rules file* parameter to point to the file you created. You need to save this file on the Data Warehouse computer, *not* the Data Mart server.

You must create the gateway rules file in the following format:

- A number sign (#) in the first column identifies a comment line.
- The rule is four fields separated by semicolons (;).
- The first field is the Gateway Name or Pattern.
- The second field is the Prefix Pattern that identifies a local call.
- The third field is the minimum number of digits that must be found in order for a call to be classified as a gateway call.
- The fourth field is the maximum number of digits that can be found in order for a call to be classified as a gateway call.



You also use this script to specify external access codes. Most systems require an access code to be dialed before routing a call to a remote or local gateway. If you specify an access code, Call Data Analysis will remove it before determining a call's classification. Keep this in mind when specifying other parameters. For example, if you want to add 1877* to the Toll Free call rules, and your external access code is 9, you need to add 1877* (not 91877*) as a pattern in the *Configure toll free call rules* parameters.

This script raises an event when the job succeeds or fails, when the Data Mart server is inaccessible, and when warnings are raised during an attempt to configure call types.

Resetting the ConfigureCallTypes Script

You can use SQL Query Analyzer on the Data Mart computer to return the parameters in the ConfigureCallTypes script to their original default values. In the **Database Selection** drop list in the Query Analyzer interface, select the Data Mart database for which you want to reset the call type rules. In the Query window, type the following command: `exec dbo.SetCallTypeDefaults`. To verify the call type rules have been reset, issue the following command in the Query window:

```
select * From CallTypesRules
```

Reviewing Call Classification Types

Use the ConfigureCallTypes Knowledge Script to configure the rules by which the Call Data Analysis module classifies the types of calls each CDR contains. The following table describes each classification type.

Classification Type	Description
Internal	Intracluster call that originated in the network and ended in the same network (no gateway was used). Both the called and calling numbers are internal numbers.
On-net	Call in which both the calling and called numbers are internal, and either the originating or destination device is a gateway.
Incoming	Call that originated outside of the network and whose called number is an internal number.
Conference bridge	Call whose destination device is a conference bridge.
Voice mail	Call whose destination device is a voice mail device.
Local	Call whose destination device is a gateway, and whose called number is not an internal number and does not have an area code (or includes one of the local area codes).
Tandem - local	Local call that originated outside of the network.
Long distance	Call whose destination device is a gateway, and whose called number is not an internal number and has an area code that is not one of the local area codes.
Tandem - long distance	Long distance call that originated outside of the network.
International	Call whose destination device is a gateway, and whose called number begins with the international access code.
Tandem - international	International call that originated outside of the network.
Tandem	If the Tandem Rule is “collapse,” this category is a combination of the Tandem - local, Tandem - long distance, and Tandem - international categories.
Service	Call to a service, usually three digits, such as 411 (Directory Service).
Emergency	Call to an emergency service, such as 911.
Toll free	Long distance call that is toll free, such as 1-800 calls.
Other	User-defined rule.
Unknown	Call that does not match any of the other categories.

Resource Objects

Call Data CallManager object

Call Data H.323 RADIUS object

Call Data CiscoCM object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Configure Call Classification Rules	
Configure External Access Code	
Action	Select whether you want to **Replace**, **Remove All**, or make **No Change** regarding the external access code. For more information, see Action Parameter. The default is Replace.
External access code	Specify the access code your system requires for routing calls to a remote or local gateway. The default is 9.
Configure Internal Call Rules	
Action	Select whether you want to **Append**, **Replace**, **Remove All**, or make **No Change** regarding internal call rules. For more information, see Action Parameter. The default is Replace.
Internal numbers or patterns	Specify numbers or patterns that identify an internal call. Separate multiple entries with a semicolon (;). The default is [2-7]xx;[1-8]xxx;[1-8]xxxxx.
Minimum digits dialed for internal calls	Specify the minimum number of digits that must be found in order for a call to be classified as internal. The default is 3.
Maximum digits dialed for internal calls	Specify the maximum number of digits that must be found in order for a call to be classified as internal. The default is 6.
Configure International Call Rules	
Action	Select whether you want to **Append**, **Replace**, or make **No Change** regarding international call rules. For more information, see Action Parameter. The default is Replace.
International dialing prefixes	Specify the prefix that identifies an international call. Do not include the external access code. The default prefixes are 011*;00*;010*. For more information, see Wildcard Characters.
Minimum digits dialed for international calls	Specify the minimum number of digits that must be found in order for a call to be classified as international. The default is 10.
Maximum digits dialed for international calls	Specify the maximum number of digits that must be found in order for a call to be classified as international. The default is 32. **Note** You can specify a large value to indicate there is no maximum limit.
Configure Local Call Rules	
Action	Select whether you want to **Replace** or make **No Change** regarding local call rules. For more information, see Action Parameter. The default is Replace.
Minimum digits dialed for local calls	Specify the minimum number of digits that must be found in order for a call to be classified as local. The default is 7.

Parameter	How to Set It
Maximum digits dialed for local calls	Specify the maximum number of digits that must be found in order for a call to be classified as local. The default is 10.
Configure Long Distance Call Rules	
Action	Select whether you want to **Replace** or make **No Change** regarding long distance call rules. For more information, see Action Parameter. The default is Replace.
Minimum digits dialed for long distance calls	Specify the minimum number of digits that must be found in order for a call to be classified as long distance. The default is 10.
Maximum digits dialed for long distance calls	Specify the maximum number of digits that must be found in order for a call to be classified as long distance. The default is 32. **Note** You can specify a large value to indicate there is no maximum limit.
Configure Long Distance Access Code	
Action	Select whether you want to **Remove All**, **Replace**, or make **No Change** regarding the long distance access code. For more information, see Action Parameter. The default is Replace.
Long distance dialing prefix	Specify the access code your system requires for routing long distance calls. The default is 1.
Configure Gateway Rules	
Action	Select whether you want to **Append**, **Remove All**, **Replace**, or make **No Change** regarding the gateway rules. For more information, see Action Parameter. The default is Remove.
Gateway Rules File	
Full path to gateway rules file	Type the fully qualified path to a file on the Data Warehouse computer that contains a list of gateway names, patterns, and prefixes that identify local calls.
Severity - File I/O problems	Set the severity level, from 1 to 40, to reflect the importance of an event in which the gateway rules file is inaccessible. The rules file could be unreachable for a number of reasons, including an incorrect fully qualified file path. The default is 20.
Gateway names or patterns	Specify the names or patterns of gateways to check. Use wildcards if necessary and use semicolons (;) to separate multiple entries. For more information, see Wildcard Characters. If you specified a gateway rules file, you do not need to complete this parameter, but you can if you have rules to add in addition to what is in the rules file.
Prefix patterns	Specify numbers or patterns that identify local calls. Use semicolons (;) to separate multiple entries. If you specified a gateway rules file, you do not need to complete this parameter, but you can if you have rules to add in addition to what is in the rules file.
Minimum digits dialed for these patterns	Specify the minimum number of digits that must be found in order for a call to fit the gateway rules. The default is 7.
Maximum digits dialed for these patterns	Specify the maximum number of digits that must be found in order for a call to fit the gateway rules. The default is 32. **Note** You can specify a large value to indicate there is no maximum limit.

Parameter	How to Set It
Configure Service Call Rules	
Action	Select whether you want to **Append**, **Remove All**, **Replace**, or make **No Change** regarding service calls. For more information, see Action Parameter. The default is Replace.
Service numbers or patterns	Specify the numbers or patterns that identify a service call. Use semicolons (;) to separate multiple entries. The default is [2-8]11.
Minimum digits dialed for service calls	Specify the minimum number of digits that must be found in order for a call to be classified as service. The default is 3.
Maximum digits dialed for service calls	Specify the maximum number of digits that must be found in order for a call to be classified as service. The default is 3.
Configure Toll Free Call Rules	
Action	Select whether you want to **Append**, **Remove All**, **Replace**, or make **No Change** regarding toll free calls. For more information, see Action Parameter. The default is Replace.
Toll free numbers or patterns	Specify the numbers or patterns that identify a toll free call. Use semicolons (;) to separate multiple entries. The default is 1800*;1855*;1866*;1877*. For more information, see Wildcard Characters.
Minimum digits dialed for toll free calls	Specify the minimum number of digits that must be found in order for a call to be classified as toll free. The default is 7.
Maximum digits dialed for toll free calls	Specify the maximum number of digits that must be found in order for a call to be classified as toll free. The default is 32. **Note** You can specify a large value to indicate there is no maximum limit.
Configure Emergency Call Rules	
Action	Select whether you want to **Append**, **Remove All**, **Replace**, or make **No Change** regarding emergency calls. For more information, see Action Parameter. The default is Replace.
Emergency numbers or patterns	Specify the numbers or patterns that identify an emergency call. Use semicolons (;) to separate multiple entries. The default is 911.
Minimum digits dialed for emergency calls	Specify the minimum number of digits that must be found in order for a call to be classified as emergency. The default is 3.
Maximum digits dialed for emergency calls	Specify the maximum number of digits that must be found in order for a call to be classified as emergency. The default is 3.
Configure Other Call Rules	
Action	Select whether you want to **Append**, **Remove All**, **Replace**, or make **No Change** regarding other calls. For more information, see Action Parameter. The default is Remove.
Other numbers or patterns	Specify the numbers or patterns that identify other calls. Use semicolons (;) to separate multiple entries.
Minimum digits dialed for other calls	Specify the minimum number of digits that must be found in order for a call to be classified as other. The default is 3.
Maximum digits dialed for other calls	Specify the maximum number of digits that must be found in order for a call to be classified as other. The default is 24. **Note** You can specify a large value to indicate there is no maximum limit.
Configure Tandem Rule	

Parameter	How to Set It
Action	Select whether you want to **Remove All** or make **No Change** regarding the tandem rule. For more information, see Action Parameter. The default is Remove All. If you remove the tandem rule, calls are not classified as tandem. In other words, all Tandem-Local, Tandem-Long Distance, and Tandem-International calls will be classified simply as Local, Long Distance, and International.
Tandem rule	Set the tandem rule as follows: • Select **Expand** to classify tandem calls as Tandem-Local, Tandem-Long Distance, and Tandem-International. The default is Expand. • Select **Collapse** to classify tandem calls as Tandem, and not split into the three sub-categories.
Update Fact Data	
Update existing fact data using updated rules?	Select **Yes** to instruct the Data Mart to update data immediately using the new or revised rules. This update does not affect the next scheduled collection.
Update previous n days of data	Specify the number of days' worth of accumulated data you want the Data Mart to update using the new or revised rules. The default is 7 day's worth of data.
Update all data?	Select **Yes** to instruct the Data Mart to update all of the data in the database. **Caution** You may have several months' or years' worth of accumulated data. Select this option only with the understanding that the process of updating a lot of data can be lengthy.
Event Notification	
Event severity when job succeeds	Set the severity level, from 1 to 40, to reflect the importance of an event in which the ConfigureCallTypes job succeeds. The default is 25.
Event severity when data mart server inaccessible	Set the severity level, from 1 to 40, to reflect the importance of an event in which the Data Mart server is inaccessible. The default is 15.
Event severity for warnings	Set the severity level, from 1 to 40, to reflect the importance of warnings raised during an attempt to configure call types. The default is 20.
Event severity when job fails	Set the severity level, from 1 to 40, to reflect the importance of an event in which the ConfigureCallTypes job fails. The default is 5.

Action Parameter

In the list of parameters, each rule and access code folder contains an Action parameter you set to indicate the action you want to take regarding the rules and access codes for each call type. The following table describes the Action options you can select.

Action Parameter Option	Description
No Change	Indicates you do not want to change the rule or access code for this call type.
Append	Appends the new rule to any existing rules for this call type.
Replace	Replaces all existing rules with the new rule you are creating for this call type.
Remove All	Removes all existing rules for this call type. If you select this option, the Call Data Analysis module does not classify calls of this type.

Wildcard Characters

When specifying number patterns in parameters, you can use any of the following wildcards and special characters.

Character	Description	Example
X	The X wildcard matches any single digit in the range of 0 through 9.	70XXX matches numbers in the range of 70000 through 70999.
*	The asterisk (*) wildcard matches one or more digits in the range of 0 through 9. **Note** You can use an exclamation point (!) in place of an asterisk.	011* matches any number beginning with 011, such as 011447968587655.
[ ]	Square brackets ([ ]) enclose a range of values.	[4578]11 matches 411, 511, 711, and 811.
-	The hyphen (-) can be used within square brackets to indicate a sequential range of values.	[4-8]11 matches 411, 511, 711, and 811.

DataCollectionStatus

Use this Knowledge Script to check the status of the last data collection job performed against a Data Source. This script raises an event when the data collection attempt fails, when the data collection job is cancelled, or when the DataCollectionStatus job itself fails.

Resource Objects

Call Data CallManager object

Call Data H.323 RADIUS object

Call Data CiscoCM object

Default Schedule

By default, this script runs daily.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Show history for previous n jobs	Specify the number of previous data collection jobs for which you want to view the status. The default is 7.
Show job steps?	Select **Yes** to enable an event to display information about each of the eight individual steps in a data-collection job. Accept the default (unselected) to display only the outcome of the job in the event. **Note** You probably do not need to see every step in a data collection job unless you are debugging a problem.
Event Notification	
Raise informational event?	Select **Yes** to raise an event that provides status information. The default is Yes.
Event severity for informational event	Set the severity level, from 1 to 40, to reflect the importance of the generation of an informational event. The default is 25.
Event severity when data collection fails	Set the severity level, from 1 to 40, to reflect the importance of an event in which the data-collection attempt fails. The default is 10. **Note** This parameter differs from *Event severity when job fails* in that it indicates the Data Mart has failed to collect data. It does not indicate the Knowledge Script itself has failed to run.
Event severity when data collection is cancelled	Set the severity level, from 1 to 40, to reflect the importance of an event in which the data collection job is cancelled. The default is 15.
Event severity when job fails	Set the severity level, from 1 to 40, to reflect the importance of an event in which the DataCollectionStatus job fails. The default is 5. **Note** This parameter differs from *Event severity when data collection fails* in that it indicates the Knowledge Script has failed to run. It does not indicate the Data Mart has failed to collect data.

ExecuteDataCollection

Use this Knowledge Script to perform on-demand data collection, regardless of the schedule. This script takes no action if data is currently being collected. Running this script does not affect the data collection schedule.

This script raises an event when the job success or fails, and when data is currently being collected.

Resource Objects

Call Data CallManager object

Call Data H.323 RADIUS object

Call Data CiscoCM object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Collection	
Start SQL Server Agent if it is stopped?	Select **Yes** to start SQL Server Agent. SQL Server Agent must be running in order for data collection tasks to be performed. The default is unselected.
Event Notification	
Event severity when job execution succeeds	Set the severity level, from 1 to 40, to reflect the importance of an event in which the ExecuteDataCollection job succeeds. The default is 25.
Event severity when job already executing	Set the severity level, from 1 to 40, to reflect the importance of a situation in which data is already being collected. The default is 25.
Event severity when job execution fails	Set the severity level, from 1 to 40, to reflect the importance of an event in which the ExecuteDataCollection job fails. The default is 5.

RemoveDataSource

Use this Knowledge Script to remove a Data Source and its associated Data Mart. This script raises an event when the removal succeeds or fails.

Tip
When this Knowledge Script job runs successfully, the Data Source object in the TreeView pane is deleted. In addition, the job itself is also deleted (a normal side-effect of removing a TreeView object). The event this job creates is not deleted because it is associated with the parent object (`CallDataAnalysis:WAREHOUSE` object). However, if you set the global preference to "Remove associated events when jobs are deleted," even the event is deleted when the object and job are deleted. To set global preferences, select **File > Preferences > Repository > Event** in the AppManager Operator Console.

Resource Objects

Call Data CallManager object

Call Data H.323 RADIUS object

Call Data CiscoCM object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source Removal	
Check following box to confirm removal	
Confirm data source removal	Select **Yes** to confirm you want to remove the Data Source. The default is unselected. This script will not run unless you set this parameter to Yes.
Delete the data mart database?	Select **Yes** to delete the database from the Data Mart computer. The default is unselected. **Note** You should not delete a database. After you delete a database, its data is lost and unavailable for use. If you do not delete the database, you can easily reconnect to it using the AddDataSource Knowledge Script.
Event Notification	
Raise event if job succeeds?	Select **Yes** to raise an event when the RemoveDataSource job succeeds. The default is Yes.
Event severity when job succeeds	Set the severity level, from 1 to 40, to reflect the importance of an event in which the RemoveDataSource job succeeds. The default is 25.
Event severity when job fails	Set the severity level, from 1 to 40, to reflect the importance of an event in which the RemoveDataSource job fails. The default is 5.

Report_CallAuthorization

Use this Knowledge Script to display the number and duration of calls that used a Forced Authorization Code (FAC) or a Client Matter Code. Both are features of Cisco Unified Communications Manager.

- An FAC is a code users must enter when attempting to make a priority phone call, such as an international call.
- A Client Matter Code is one users must enter to assign a phone call to a particular billing entity, such as a specific client or project.

This report supports only Unified Communications Manager Data Sources.

Identifying Unauthorized Usage

Your organization may use Forced Authorization Codes and Client Matter Codes to allow your employees to make long distance calls based on business need. However, authorization codes have a way of being shared. You can monitor authorization code usage with the Report_CallAuthorization Knowledge Script.

Let us say your billing records indicate a client account has been charged for what seems like excess telephone calls. Using Report_CallAuthorization, set the *Show calls by* parameter to **ClientMatterCode**. Set the *Show details by* parameter to **CallingLocation**. Your report will display a chart that groups calls by Client Matter Code and calling location, allowing you to easily identify which calling location is making the excess charges.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source(s)	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Minimum duration	Specify the minimum duration filter for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. The default is 0 seconds.
Show calls by	Select the delimiter by which you want to group the calls in your report. You can choose from the following sorting options: • **FAC Level** • **FAC Name** • **Client Matter Code**

Parameter	How to Set It
Show details by	Select the details you want to show for each group of calls. You can choose from the following detail options: • **CallManager Cluster** • **Calling Partition** • **Called Partition** • **Calling Location** • **Called Location** • **Outbound Trunk Group** • **Inbound Trunk Group** • **Outbound Gateway** • **Inbound Gateway** • **Hour of Day** • **Day of Week** • **None**. If you select None, no time details are shown.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Units for chart	Select the unit of measurement that should appear on the Y axis of the chart: **Duration** or **Number Of Calls**. The default is Number of Calls. If you select Duration, the duration unit measurement is determined by the value you select in the *Show duration in Erlangs or seconds?* parameter.

Show duration in Erlangs or seconds?	Select whether you want the duration measurement to display in **Erlangs** or **Seconds**. The default is Erlangs.
	Also known as a traffic unit, an Erlang is a measurement of traffic load during the busy hour, and is based on having 3600 seconds (60 minutes or one hour) of calls on the same circuit, trunk, or port. (In other words, one circuit is busy for one hour regardless of the number of calls or the average length of calls). For example, if a call center received 30 six-minutes calls in the busy hour, it received 180 call minutes, or three Erlangs. If a call center received 100 calls that averaged 36 seconds in the busy hour, it received 3600 call seconds or one Erlang.
	You can use the following formula to calculate an Erlang value:
	`Traffic in Erlangs =`
	`(Number of calls in the busy hour) * (AHT seconds)/3600`

Include “Unassigned” in summary chart?	Set to **y** to include all calls for which no FAC or Client Matter Code was used. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CallAuthorization.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Call Authorization.

Parameter	How to Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event if the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_CallCompletionRate

Use this Knowledge Script to determine the completion rate of calls recorded with the selected Data Source. The call completion rate takes into account failed calls (determined by the disconnect cause code) and abandoned calls (calls with a successful disconnect cause code, but having a duration of zero).

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source(s)	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.

Parameter	How to Set It
Group by	Select the delimiter by which you want to group the calls in your report. You can choose from the following sorting options: • **Data Publisher**. Choose this option to sort the report by the entity that generates the data: Communications Manager Publisher, Communications Manager primary server, or RADIUS gateway. • **Calling Partition** (applies to Communications Manager Data Sources) • **Called Partition** (applies to Communications Manager Data Sources) • **Calling Location** (applies to Communications Manager Data Sources) • **Called Location** (applies to Communications Manager Data Sources) • **Outbound Trunk Group** (applies to Communications Manager Data Sources) • **Inbound Trunk Group** (applies to Communications Manager Data Sources) • **Outbound Gateway** (applies to all Data Sources) • **Inbound Gateway** (applies to all Data Sources) • **CallManager Cluster**. This option provides the same sorting results as Data Publisher. This option is maintained in the script to provide backwards compatibility to older versions of AppManager for Call Data Analysis. • **None**. Choose this option to combine all calls into a single group. **Note** If your *Select data source(s)* and *Group by* selections are incompatible (perhaps you selected an H.323 Data Source and a Communications Manager grouping), the report ignores your *Group by* selection and uses the default selection, which is Data Publisher.
Show time details by	Select the time details you want to show for each group of calls. You can choose from the following detail options: • **Hour of Day** • **Day of Week** • **Day of Month** • **None**. If you select None, no time details are shown.
Exclude these failure codes	Type a list of termination codes (separated by commas) that are not to be considered failures. See Termination Codes for a list of available codes. **Note** Codes 0, 16, 31, and 127 are automatically excluded. They are normal termination codes. However, these codes may appear in events if the other side of the call has a failure code that has not been excluded.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CallDataCompletionRate.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.

Parameter	How to Set It
Select properties	Set miscellaneous report properties as desired. The default report name is Call Completion Rate.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event if the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_CallDetail_CiscoCallMgr

Use this Knowledge Script to display details for calls that match criteria you specify for a selected Unified Communications Manager. Call details can include time, calling number, and called number. Any criteria parameter you leave blank is not included in the search.

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Identifying Malicious Calls

This report can aid you in identifying malicious calls for a VoIP security assessment. Your company may have its own definition of what constitutes a malicious call, but in general, a malicious call is disturbing or harmful to the recipient. Examples of malicious calls include incoming fax calls, calls from telemarketers, or calls from external recruiters.

Cisco Unified Communications Manager provides a Malicious Call ID feature. When configured, this feature allows a user to identify a malicious call by pressing a soft key. Communications Manager stores information about the unwanted call in the CDR database. AppManager can filter the CDR database for any call flagged as malicious.

Using the Report_CallDetail_CiscoCallMgr Knowledge Script and the *Calls identified as malicious* parameter, you can create a report that identifies the time, number, and IP address of the malicious caller. By also specifying a **CalledNumber** or **CallingNumber** in the *Search Criteria* parameter, you can filter the report to display all malicious calls to or from a particular number.

Let us say your engineers were being plagued with calls from an outside recruiter. They identified the calls as malicious and you ran Report_CallDetails to pinpoint the calling number. After you identified the malicious calling number, you routed future calls from this number through your voice gateway to your main phone operator. Your operator quickly dispatched the recruiter and your engineers returned to their work.

What if one of your employees receives a disturbing or malicious call, but is using a phone that is not equipped to flag a malicious call? You can use the Report_CallDetails Knowledge Script and the time of the call to create a report that displays all calls within a certain time period. Use the *Select time range* parameter to indicate the time of the call. Then supply the employee's phone number in the *Search criteria - Called number* parameter. AppManager will search the CDR database for all calls to the employee's number that occurred during the period you specified.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Minimum duration	Specify a minimum duration for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. Type 0 to indicate no limit.
Maximum duration	Specify a maximum duration for calls selected by the script. Calls with a duration of greater than the maximum will not be included in the report, even if all other criteria are satisfied. Type 0 to indicate no limit.
Search Criteria	
Note for entering search criteria: If you specify only the wildcard (*) for a field (such as calling number), AppManager matches *only* those calls that have a value for that field. Calls for which that field has no value (i.e., is NULL) will not be matched. For example, if you specify * in the “Calling partition name” parameter, the search matches only those calls that have some partition name configured. To match all calls (including calls that have no value for the selected field), leave the search criteria parameter blank.	
Calling number	Specify the calling number you want to find.
Called number	Specify the called number you want to find.
Calling device name	Specify the name of the calling device you want to find.
Called device name	Specify the name of the called device you want to find.
Calling device IP address	Specify the IP addresses of the calling devices you want to find. Use one of the following formats: • Single dotted-decimal IP address, such as 10.41.2.31 • Dotted-decimal IP address that includes a wildcard, such as 10.41.*.*, which would search for all IP addresses in the range of 10.41.0.0 to 10.41.255.255. • Range of dotted-decimal IP addresses separated by a hyphen, such as 10.41.2.31-10.41.2.41. The first address indicates the beginning of the range; the second IP address marks the end of the range.
Called device IP address	Specify the IP addresses of the called devices you want to find. Use one of the following formats: • Single dotted-decimal IP address, such as 10.41.2.31 • Dotted-decimal IP address that includes a wildcard, such as 10.41.*.*, which would search for all IP addresses in the range of 10.41.0.0 to 10.41.255.255. • Range of dotted-decimal IP addresses separated by a hyphen, such as 10.41.2.31-10.41.2.41. The first address indicates the beginning of the range; the second IP address marks the end of the range.
Calling device location name	Specify the name of the calling device location you want to find. Use the location configured on the Communications Manager.

Parameter	How to Set It
Called device location name	Specify the name of the called device location you want to find. Use the location configured on the Communications Manager.
Calling partition name	Specify the name of the calling partition you want to find.
Called partition name	Specify the name of the called partition you want to find.
Inbound trunk group name	Specify the name of the inbound trunk group you want to find.
Outbound trunk group name	Specify the name of the outbound trunk group you want to find.
Calls identified as malicious	Select **Yes** to search for calls identified as malicious by call recipients. The default is unselected.
Forced Authorization Code (FAC) level or range of levels	Specify the FAC level you want to find. Specify a single FAC level, such as `30`, or a range of levels separated by a hyphen, such as `30-50`. The maximum level is 255. To search for all levels above a certain point, specify a range that begins with the certain point and ends with 255, such as `30-255`. **Note** An FAC is a code users must enter when attempting to make a priority phone call, such as an international call.
Forced Authorization Code (FAC) name	Specify the FAC name you want to find. An FAC is a code users must enter when attempting to make a priority phone call, such as an international call. The text string can contain the ***** wildcard.
Client Matter Code	Specify the client matter code you want to find. A client matter code is one users must enter to assign a phone call to a particular billing entity, such as a specific client or project. The text string can contain the ***** wildcard.
Comment field	Specify a string of text you want to find in the CDR Comment field. The text string can contain the ***** wildcard.
Call Details to Include in Report	
Call duration	Select to include call duration in the call details for each call in the report. The default is checked.
Call type	Select to include call classification type in the call details for each call in the report. The default is unselected. For more information, see “Reviewing Call Classification Types” on page 696.
Originator disconnect cause code	Select to include the disconnect cause code in the call details for each originator call included in the report. The default is checked.
Destination disconnect cause code	Select to include the disconnect cause code in the call details for each destination call included in the report. The default is checked.
Call ID	Select to include the call ID in the call details for each call in the report. The default is unselected. The call ID is a globally unique identifier (GUID) that identifies the call. AppManager uses the call ID from the pkid field in the CallDetailRecord table in the Communications Manager CDR database.
Partition and Device Information	
Calling number partition name	Select to include the name of the calling number partition in the call details for each call in the report. The default is unselected.
Calling device location name	Select to include the name of the calling device location in the call details for each call in the report. Use the location configured on the Communications Manager. The default is unselected.
Originator IP address	Select to include the IP address of the originating phone in the call details for each call in the report. The default is unselected.

Parameter	How to Set It
Originator device name	Select to include the name of the originating device in the call details for each call in the report. The default is unselected.
Originator media IP address	Select to include the IP address of the device that originated the media for the call. • For Cisco IP calls, this selection returns the address of the Cisco IP phone. • For PSTN calls, this selection returns the address of the gateway. • For intercluster calls, this selection returns the address of the remote Cisco IP phone.
Originator media port	Select to include the IP port number associated with the originating media IP address.
Inbound trunk group name	Select to include the name of the inbound trunk group in the call details for each call in the report. The default is unselected. **Note** This parameter is applicable only when a gateway is involved.
Called number partition name	Select to include the name of the called number partition in the call details for each call in the report. The default is unselected.
Called device location name	Select to include the name of the called device location in the call details for each call in the report. Use the location configured on the Communications Manager. The default is unselected.
Destination IP address	Select to include the IP address of the destination phone in the call details for each call in the report. The default is unselected.
Destination device name	Select to include the name of the destination device in the call details for each call in the report. The default is unselected.
Destination media IP address	Select to include the IP address of the device that terminated the media for the call. • For Cisco IP calls, this selection returns the address of the Cisco IP phone. • For PSTN calls, this selection returns the address of the H.323 gateway. • For intercluster calls, this selection returns the address of the remote Cisco IP phone.
Destination media port	Select to include the IP port number associated with the destination media IP address.
Outbound trunk group name	Select to include the name of the outbound trunk group in the call details for each call in the report. The default is unselected. **Note** This parameter is applicable only when a gateway is involved.
Quality Metrics	
Originator ...	Select to include one or more originating phone metrics in the call details for each call in the report. The default is unselected. • **Codec type** • **Jitter** • **Latency**
Destination ...	Select to include the following destination phone metrics in the call details for each call in the report. The default is unselected. • **Codec type** • **Jitter** • **Latency**
Listening MOS	

Parameter	How to Set It
Originator ...	Select to include one or more MOS-related (Mean Opinion Score) originating phone metrics in the call details for each call in the report. The default is unselected. • **Average MOS** • **Minimum MOS** • **Maximum MOS** • **Last MOS**
Destination ...	Select to include one or more MOS-related (Mean Opinion Score) destination phone metrics in the call details for each call in the report. The default is unselected. • **Average MOS** • **Minimum MOS** • **Maximum MOS** • **Last MOS**
Packets	
Originator ...	Select to include one or more packet-related originating phone metrics in the call details for each call in the report. The default is unselected. • **Packets sent** • **Packets received** • **Packets lost**
Destination ...	Select to include one or more packet-related destination phone metrics in the call details for each call in the report. The default is unselected. • **Packets sent** • **Packets received** • **Packets lost**
Concealment	
Originator ...	Select to include one or more concealment-related originating phone metrics in the call details for each call in the report. Concealment metrics measure packet (frame) loss and its effect on voice quality in an impaired network. The default is unselected. • **Cumulative conceal ratio**, the cumulative ratio of concealment time over speech time observed after starting a call. • **Interval conceal ratio**, an interval-based average concealment rate, is the ratio of concealment time over speech time for the last three seconds of active speech. • **Maximum conceal ratio**, the maximum concealment ratio observed during a call. • **Conceal seconds**, the amount of time during which some concealment is observed during a call. • **Severely conceal seconds**, the amount of time during which a significant amount of concealment is observed. If the concealment observed is usually greater than 50 milliseconds or approximately 5%, the speech is probably not very audible.

Parameter	How to Set It
Destination ...	Select to include one or more concealment-related destination phone metrics in the call details for each call in the report. Concealment metrics measure packet (frame) loss and its effect on voice quality in an impaired network. The default is unselected. • **Cumulative conceal ratio**, the cumulative ratio of concealment time over speech time observed after starting a call. • **Interval conceal ratio**, an interval-based average concealment rate, is the ratio of concealment time over speech time for the last three seconds of active speech. • **Maximum conceal ratio**, the maximum concealment ratio observed during a call. • **Conceal seconds**, the amount of time during which some concealment is observed during a call. • **Severely conceal seconds**, the amount of time during which a significant amount of concealment is observed. If the concealment observed is usually greater than 50 milliseconds or approximately 5%, the speech is probably not very audible.
Security Information	
Forced Authorization Code (FAC) level	Select to include the FAC level in the call details for each call in the report. The default is unselected.
Forced Authorization Code (FAC) name	Select to include the FAC name in the call details for each call in the report. The default is unselected.
Client Matter Code	Select to include the client matter code in the call details for each call in the report. The default is unselected.
Comment field	Select to include the contents of the CDR Comment field in the call details for each call in the report. The default is unselected.
Report Settings	
Maximum number of calls to return	Specify the maximum number of calls to include in the report. The default is 1000 calls. **Note** No matter how many calls you choose to include in the call details section of the report, the report will also include a small table that indicates how many calls actually met your search criteria. This number may, and probably will, exceed the number of calls you choose to return.

Parameter	How to Set It
Order rows by?	Select one of the following call detail options as the criterion for sorting the rows in the report: • **Ascending Time** (oldest to most recent) • **Descending Time** (most recent to oldest) • **Longest Duration** (longest to shortest) • **Shortest Duration** (shortest to longest) • **Calling Number** • **Called Number** • **Calling Partition**. If you select this option, you must also check the Calling number partition name parameter under the Partition and device information section of this script. • **Called Partition**. If you select this option, you must also check the Called number partition name parameter under the Partition and Device Information section of this script. • **Calling Location**. If you select this option, you must also check the Calling device location name parameter under the Partition and Device Information section of this script. • **Called Location**. If you select this option, you must also check the Called device location name parameter under the Partition and Device Information section of this script. • **Ascending FAC Level** (lowest to highest number) • **Descending FAC Level** (highest to lowest number) • **FAC Name** • **Client Matter Code**
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is CallDataDetails.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Call Details.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event if the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_CallDetail_H323Gateway

Use this Knowledge Script to display details for calls that match criteria you specify for a selected H.323 gateway. Call details can include time, calling number, and called number. Any criteria parameter you leave blank is not included in the search.

If you have Cisco Communications Manager Express gateways, run CCME_GetConfig to ensure the Data Collection process has access to configuration information when processing call detail records. Without the configuration information, the Data Collection process cannot determine the IP address of the Communications Manager Express phone and you will not be able to use the *Originating IP Address* and *Terminating IP Address* selection parameters in this Report script.

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Minimum duration	Specify a minimum duration for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. Type 0 to indicate no limit.
Maximum duration	Specify a maximum duration for calls selected by the script. Calls with a duration of greater than the maximum will not be included in the report, even if all other criteria are satisfied. Type 0 to indicate no limit.
Search Criteria	
Note for entering search criteria: If you specify only the wildcard (*) for a field (such as calling number), AppManager matches *only* those calls that have a value for that field. Calls for which that field has no value (i.e., is NULL) will not be matched. For example, if you specify * in the *Calling partition name* parameter, the search matches only those calls that have some partition name configured. To match all calls (including calls that have no value for the selected field), leave the search criteria parameter blank.	
Calling number	Specify the calling number you want to find.

Parameter	How to Set It
Called number	Specify the called number you want to find.
Originating gateway name	Specify the name of the originating gateway you want to find.
Terminating gateway name	Specify the name of the terminating gateway you want to find.
Originating IP address	Specify the IP addresses of the originating gateways you want to find. Use one of the following formats: • Single dotted-decimal IP address, such as 10.41.2.31 • Dotted-decimal IP address that includes a wildcard, such as 10.41.*.*, which would search for all IP addresses in the range of 10.41.0.0 to 10.41.255.255. • Range of dotted-decimal IP addresses separated by a hyphen, such as 10.41.2.31-10.41.2.41. The first address indicates the beginning of the range; the second IP address marks the end of the range. For calls through the gateway from the PSTN, this search criterion returns the actual IP address of the gateway. For calls through the gateway from Communications Manager Express phones, this search criterion returns the IP address of the Communications Manager Express phones. If this IP address cannot be determined from Communications Manager Express configuration information, this search criterion returns no information.
Terminating IP address	Specify the IP addresses of the terminating gateways you want to find. You can use one of the following formats: • Single dotted-decimal IP address, such as 10.41.2.31 • Dotted-decimal IP address that includes a wildcard, such as 10.41.*.*, which would search for all IP addresses in the range of 10.41.0.0 to 10.41.255.255. • Range of dotted-decimal IP addresses separated by a hyphen, such as 10.41.2.31-10.41.2.41. The first address indicates the beginning of the range; the second IP address marks the end of the range. For calls through the gateway to the PSTN, this search criterion returns the actual IP address of the gateway. For calls through the gateway to Communications Manager Express phones, this search criterion returns the IP address of the Communications Manager Express phones. If this IP address cannot be determined from Communications Manager Express configuration information, this search criterion returns no information.
Inbound trunk group name	Specify the name of the inbound trunk group you want to find.
Outbound trunk group name	Specify the name of the outbound trunk group you want to find.
Call Details to Include in Report	
Call duration	Select to include call duration in the call details for each call in the report. The default is checked.
Call type	Select to include call classification type in the call details for each call in the report. The default is unselected. For more information, see “Reviewing Call Classification Types” on page 696.
Originating gateway disconnect cause code	Select to include the disconnect cause code in the call details for each originating gateway call included in the report. The default is checked.
Terminating gateway disconnect cause code	Select to include the disconnect cause code in the call details for each terminating gateway call included in the report. The default is checked.

Parameter	How to Set It
Call ID	Select to include the call ID in the call details for each call in the report. The default is unselected. The call ID is a globally unique identifier (GUID) that identifies the call. AppManager uses the call ID from the h323-conf-id field received in the RADIUS records; all H.323 call legs belonging to the same call will have the same h323-conf-id.
Gateway, Port, and IP Information	
Originating gateway name	Select to include the name of the originating gateway in the call details for each call in the report. The default is unselected.
Originating gateway voice port	Select to include the port number of the originating gateway voice port in the call details for each call in the report. The default is unselected.
Originating IP address	Select to include the IP address of the originating gateway or Communications Manager Express phone in the call details for each call in the report. The default is unselected.
Inbound trunk group name	Select to include the name of the inbound trunk group in the call details for each call in the report. The default is unselected.
Terminating gateway name	Select to include the name of the terminating gateway in the call details for each call in the report. The default is unselected.
Terminating gateway voice port	Select to include the port number of the terminating gateway voice port in the call details for each call in the report. The default is unselected.
Terminating IP address	Select to include the IP address of the terminating gateway or Communications Manager Express phone in the call details for each call in the report. The default is unselected.
Outbound trunk group name	Select to include the name of the outbound trunk group in the call details for each call in the report. The default is unselected.
Quality Metrics	
Originating gateway ...	Select to include the following originating gateway metrics in the call details for each call in the report. The default is unselected. • **Codec type** • **MOS** • **R-value** • **ICPIF Voice Quality** • **Packets sent** • **Packets received** • **Packets lost** • **Packets early** • **Packets late** • **Delay**

Parameter	How to Set It
Terminating gateway ...	Select to include the following terminating gateway metrics in the call details for each call in the report. The default is unselected. • **Codec type** • **MOS** • **R-value** • **ICPIF Voice Quality** • **Packets sent** • **Packets received** • **Packets lost** • **Packets early** • **Packets late** • **Delay**
Remote Session Protocol and IP Addresses	
Originating gateway session protocol	Select to include the protocol being used on the originating VoIP legs of a call. Cisco voice gateways set this information to “cisco” for the H.323 protocol.
Originating gateway remote gateway IP address	Select to include the IP address of the originating gateway’s terminating gateway in the call details for each call in the report. The default is unselected. For a call coming in through the voice gateway to an IP phone registered to a Communications Manager, the remote gateway IP address is that of the Communications Manager.
Originating gateway remote gateway port	Select to include the port number of the originating gateway’s terminating gateway in the call details for each call in the report. The default is unselected. For a call coming in through the voice gateway to an IP phone registered to a Communications Manager, the remote gateway port is that of the Communications Manager.
Originating gateway remote media IP address	Select to include the IP address of the originating gateway’s remote media in the call details for each call in the report. The default is unselected. The remote media address is the IP address to which media is streamed. For a call coming in through the voice gateway to an IP phone registered to a Communications Manager, the remote media IP address is that of the phone.
Originating gateway remote media port	Select to include the port number of the originating gateway’s terminating media in the call details for each call in the report. The default is unselected. For a call coming in through the voice gateway to an IP phone registered to a Communications Manager, the remote gateway port is that of the phone.
Terminating gateway session protocol	Select to include the protocol being used on the terminating VoIP legs of a call. Cisco voice gateways set this information to “cisco” for the H.323 protocol.
Terminating gateway remote gateway IP address	Select to include the IP address of the terminating gateway’s originating gateway in the call details for each call in the report. The default is unselected. For a call leaving the voice gateway from an IP phone registered to a Communications Manager, the originating gateway IP address is that of the Communications Manager.

Parameter	How to Set It
Terminating gateway remote gateway port	Select to include the port number of the terminating gateway's originating gateway in the call details for each call in the report. The default is unselected. For a call leaving the voice gateway from an IP phone registered to a Communications Manager, the originating gateway port is that of the Communications Manager.
Terminating gateway remote media IP address	Select to include the IP address of the terminating gateway's remote media in the call details for each call in the report. The default is unselected. The remote media address is the IP address to which media is streamed. For a leaving the voice gateway from an IP phone registered to a Communications Manager, the remote media IP address is that of the phone.
Terminating gateway remote media port	Select to include the port number of the terminating gateway's originating media port in the call details for each call in the report. The default is unselected. For a call leaving the voice gateway from an IP phone registered to a Communications Manager, the remote media port is that of the phone.
Report Settings	
Maximum number of calls to return	Specify the maximum number of calls to include in the report. The default is 1000 calls. **Note** No matter how many calls you choose to include in the call details section of the report, the report will also include a small table that indicates how many calls actually met your search criteria. This number may, and probably will, exceed the number of calls you choose to return.
Order rows by?	Select one of the following call detail options as the criterion for sorting the rows in the report: • Ascending Time (oldest to most recent) • Descending Time (most recent to oldest) • Longest Duration (longest to shortest) • Shortest Duration (shortest to longest) • Calling Number • Called Number • Orig Gateway Name. If you select this option, also check the Originating gateway name parameter under the Gateway and Port information folder of this script. • Term Gateway Name. If you select this option, also check the Terminating gateway name parameter under the Gateway and Port Information folder of this script. • Inbound Trunk Group. If you select this option, also check the Inbound trunk group name parameter under the Gateway and Port information folder of this script. • Outbound Trunk Group. If you select this option, also check the Outbound trunk group name parameter under the Gateway and Port information folder of this script.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is CallDetail_H323Gateway.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.

Parameter	How to Set It
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco H.323 Gateway Call Details.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event if the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_CallFailureCauses

Use this Knowledge Script to analyze the failure causes for calls matching criteria you specify. You can select more than one filter in the Search Criteria parameters.

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Exclude these failure codes	Specify a list of termination codes (separated by commas) that are not to be considered failures. See Termination Codes for a list of available codes. **Note** Codes 0, 16, 31, and 127 are automatically excluded. They are normal termination codes. However, these codes may appear in events if the other side of the call has a failure code that has not been excluded.
Minimum duration	Specify the minimum duration filter for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. The default is 0 seconds.
Search Criteria	
Note for entering search criteria: If you specify only the wildcard (*) for a field (such as calling number), AppManager matches *only* those calls that have a value for that field. Calls for which that field has no value (i.e., is NULL) will not be matched. For example, if you specify * in the *Calling partition name* parameter, the search matches only those calls that have some partition name configured. To match all calls (including calls that have no value for the selected field), leave the search criteria parameter blank.	
Calling number	Specify the calling number you want to find.
Called number	Specify the called number you want to find.
Calling device name	Specify the name of the calling device you want to find.
Called device name	Specify the name of the called device you want to find.

Parameter	How to Set It
Calling device IP address	Specify the IP addresses of the calling devices you want to find. Use one of the following formats: • Single dotted-decimal IP address, such as 10.41.2.31 • Dotted-decimal IP address that includes a wildcard, such as 10.41.*.*, which would search for all IP addresses in the range of 10.41.0.0 to 10.41.255.255. • Range of dotted-decimal IP addresses separated by a hyphen, such as 10.41.2.31-10.41.2.41. The first address indicates the beginning of the range; the second IP address marks the end of the range.
Called device IP address	Specify the IP addresses of the called devices you want to find. Use one of the following formats: • Single dotted-decimal IP address, such as 10.41.2.31 • Dotted-decimal IP address that includes a wildcard, such as 10.41.*.*, which would search for all IP addresses in the range of 10.41.0.0 to 10.41.255.255. • Range of dotted-decimal IP addresses separated by a hyphen, such as 10.41.2.31-10.41.2.41. The first address indicates the beginning of the range; the second IP address marks the end of the range.
Calling device location name	Specify the name of the calling device location you want to find. Use the location configured on the Communications Manager.
Called device location name	Specify the name of the called device location you want to find. Use the location configured on the Communications Manager.
Calling partition name	Specify the name of the calling partition you want to find.
Called partition name	Specify the name of the called partition you want to find.
Inbound trunk group name	Specify the name of the inbound trunk group you want to find.
Outbound trunk group name	Specify the name of the outbound trunk group you want to find.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include time details table?	Set to **y** to include the time details table in the report. The time details table presents a breakdown of the failure causes that occurred during each hour of the reporting period.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Pie.
Select output folder	Set parameters for the output folder. The default folder name is CallDataFailureCauses.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Call Failure Causes.

Parameter	How to Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event if the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Termination Codes

Use this list of termination codes (also known as call release cause codes) to complete the *Exclude these failure codes* parameter.

Termination Code	Description	Explanation
0	No error	No error.
1	Unallocated (unassigned) number	Indicates the called party cannot be reached because, although the called party number is in a valid format, it is not currently allocated (assigned).
2	No route to specified transit network (national use)	Indicates one of the following: • The equipment sending this code has received a request to route the call through a transit network it does not recognize. The equipment does not recognize the transit network either because the transit network does not exist or because the transit network exists but does not serve the equipment sending the code. • The prefix 0 is invalid for the entered number.
3	No route to destination	Indicates one of the following: • The called party cannot be reached because the network through which the call has been routed does not service the desired destination. This cause is supported on a network-dependent basis. • A 1 was dialed when not required. Redial without the 1.
4	Send special information tone	Indicates one of the following: • The prefix 1 is not required for this number. • The called party cannot be reached for reasons of a long-term nature. The special information tone should be returned to the calling party.
5	Misdialed trunk prefix (national use)	Indicates the erroneous inclusion of a trunk prefix in the called party number.

Termination Code	Description	Explanation
6	Channel unacceptable	Indicates a called user cannot negotiate for a B-channel other than that specified in the SETUP message.
7	Call awarded and being delivered in an established channel	Indicates the user has been awarded the incoming call and the call is being connected to a channel (such as packet mode or X.25 virtual calls) already established to that user for similar calls.
8	Preemption	Indicates a call has been preempted.
9	Preemption - circuit reserved for reuse	Indicates a call has been preempted because the circuit is reserved for reuse.
16	Normal call clearing	Indicates normal call clearing has occurred.
17	User busy	Indicates the called party is unable to accept another call because the user busy condition has been encountered. Code 17 may be generated by the called user or by the network. In the case of user-determined user busy, it is noted that the user equipment is compatible with the call.
18	No user responding	Indicates a called party does not respond to a call establishment message with an alerting or connect indication within the allotted prescribed period of time (before timer T303 or T310 has expired).
19	No answer from user (user alerted)	Indicates the called user has provided an alerting indication, but not a connect indication within a prescribed period of time (before timer T301 has expired).
20	Subscriber absent	Indicates one of the following:· • A mobile station has logged off. • Radio contact is not obtained with a mobile station. • A personal telecommunications user is temporarily not addressable at any user-network interface.
21	Call rejected	Indicates one of the following: • The equipment sending this cause does not want to accept the call, although it could have accepted the call because it is neither busy nor incompatible. • May be generated by the network, indicating the call was cleared due to a supplementary service constraint.
22	Number changed	Indicates the called party number indicated by the calling party is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this cause, cause #1 shall be used.
26	Non-selected user clearing	Indicates the user has not been awarded the incoming call.
27	Destination out of order	Indicates the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" indicates a signal message was unable to be delivered to the remote party, as in the following examples: • Physical layer or data link layer failure at the remote party • User equipment off-line

Termination Code	Description	Explanation
28	Invalid number format (address incomplete)	Indicates one of the following: • The called party cannot be reached because the called party number is not in a valid format or is not complete. • The user should be returned a Special Intercept Announcement.
29	Facility rejected	Indicates one of the following: • The network cannot provide the requested facility. • A user in a special business group, such as a Centrex, dialed an undefined code.
30	Response to STATUS ENQUIRY	Indicates one of the following: • This cause is included in the Status Message when the reason for sending the Status Message was the previous receipt of a Status Enquiry message. • A user from outside a basic business group, such as a Centrex, has violated an access restriction feature.
31	Normal, unspecified	Used to report a normal event only when no other cause in the normal class applies.
34	No circuit/channel available	Indicates no appropriate circuit or channel is available to handle the call.
38	Network out of order	Indicates the network is not functioning correctly and the condition is likely to last a relatively long time. Immediately re-attempting the call is not likely to be successful.
39	Permanent frame mode connection out of service	Indicates a permanent connection was terminated, probably due to equipment failure.
40	Permanent frame mode connection operational	Indicates a permanent connection is operational again. The connection was previously terminated, probably due to equipment failure.
41	Temporary failure	Indicates the network is not functioning correctly and the condition is not likely to last a long time. The user may want to attempt another call almost immediately. May also indicate a data link layer malfunction locally or at the remote network interface, or a call was cleared due to protocol error(s) at the remote network interface.
42	Switching equipment congestion	Indicates the switching equipment generating this cause is experiencing a period of high traffic.
43	Access information discarded	Indicates the network is unable to deliver user information (such as user-to-user information, low-level compatibility, or sub-address) to the remote users as requested.
44	Requested circuit/channel not available	Indicates the other side of the interface cannot provide the circuit or channel indicated by the requesting entity.
46	Precedence call blocked	Indicates the remote device that was called is busy.
47	Resource unavailable, unspecified	Indicates one of the following: • No other cause in the resource unavailable class applies. • The original destination is unavailable. Invoke redirection to a new destination.
49	Quality of Service not available	Indicates the network cannot provide the requested Quality of Service. May be a subscription problem.

Termination Code	Description	Explanation
50	Requested facility not subscribed	Indicates this facility is unavailable because the user has not subscribed to it.
53	Service operation violated	Indicates the user has violated the service operation.
54	Incoming calls barred	Indicates the user will not accept the call delivered in the SETUP message.
55	Incoming calls barred within Closed User Group (CUG)	Indicates the network does not allow the user to receive calls.
57	Bearer capability not authorized	Indicates the user has requested a bearer capability implemented by the equipment that generated this cause. However, the user is not authorized to use it. This common problem is caused by incorrect Telco provisioning of the line at the time of installation.
58	Bearer capability not presently available	Indicates the user has requested a bearer capability implemented by the equipment that generated this cause. However, bearer capability is unavailable at the present time. This problem may be due to a temporary network problem or a subscription problem.
62	Inconsistency in designated outgoing access information and subscriber class	Indicates an inconsistency in the designated outgoing access information and subscriber class.
63	Service or option not available, unspecified	Indicates a service or option is not available. Used only when no other cause in this class applies.
65	Bearer capability not implemented	Indicates the equipment sending this cause does not support the requested bearer capability.
66	Channel type not implemented	Indicates the called party has reached an unsupported channel type.
69	Requested facility not implemented	Indicates the network (or node) does not support the requested bearer capability and therefore cannot be accessed at this time.
70	Only restricted digital information bearer capability available (national use)	Indicates the calling party has requested an unrestricted bearer service. However, the equipment sending this cause supports only the restricted version of the requested bearer capability.
79	Service or option not implemented, unspecified	Indicates a service or option was not implemented. Used only when no other cause in this class applies.
81	Invalid call reference value	Indicates the equipment sending this cause has received a message with a call reference not currently in use on the user-network interface. This value applies only if the call reference value is 1 or 2 octets long and is not the global call reference.
82	Identified channel does not exist	Indicates the equipment sending this cause has received a request to use a channel not active on the interface for a call.
83	A suspended call exists, but this call identity does not	Indicates a suspended call exists but the call's identity does not.
84	Call identity in use	Indicates a call identity is in use.
85	No call suspended.	Indicates no call is suspended.
86	Call having the requested call identity has been cleared	Indicates the call having the requested call identity has cleared.

Termination Code	Description	Explanation
87	User not member of Closed User Group (CUG)	Indicates the call was not completed, probably due to one of the following reasons: • The dialed number is incorrect • The user is not authorized to use (or has not subscribed to) the requested service • User is using a service the remote device is not authorized to use
88	Incompatible destination	Indicates the equipment sending this cause has received a request to establish a call that has low layer compatibility, high layer compatibility, or other compatibility attributes (such as data rate or DN subaddress), which cannot be accommodated. This call can be returned by a switch to a CPE when trying to route a call to an incompatible facility, or one without a data rate.
90	Destination number missing and DC not subscribed	Indicates the call was not completed, probably due to one of the following reasons: • The dialed number is incorrect • The user is not authorized to use (or has not subscribed to) the requested service • User is using a service the remote device is not authorized to use
91	Invalid transit network selection (national use)	Indicates an invalid transit network selection has been requested.
95	Invalid message, unspecified	Indicates the entity sending this cause has received an invalid message. Used when no other cause in this class applies.
96	Mandatory information element is missing	Indicates the equipment sending this cause has received a message that is missing an information element that must be present in the message before the message can be processed.
97	Message type non-existent or not implemented	Indicates one of the following: • The equipment sending this cause has received a message type it does not recognize. Either the message is not defined, or it is defined and not implemented by the equipment sending this cause. • A problem with the remote configuration or with the local D-channel.
98	Message not compatible with the call state, or the message type is non-existent or not implemented	Indicates one of the following: • Message received is not compatible with the call state • Message type is non-existent or not implemented
99	An information element or parameter non-existent or not implemented	Indicates the equipment sending this cause has received a message that includes information elements not recognized because either the information element identifier is not defined, or it is defined but not implemented by the equipment sending the cause. However, the information element is not required for the equipment sending the cause to process the message.
100	Invalid information element contents	Indicates the equipment sending this cause has received an information element it has implemented. However, one or more fields of the information elements are coded in such a way (such as truncated, invalid extension bit, invalid field values) that the information element has not been implemented by the equipment sending this cause.

Termination Code	Description	Explanation
101	The message not compatible with the call state	Indicates one of the following: • The equipment sending this cause has received a message that procedures indicate is not a permissible message to receive at this time. • The switch sending this cause is clearing the call because a threshold has been exceeded for multiple protocol errors during an active call.
102	Call terminated when timer expired; a recovery routine executed to recover from the error	Indicates a procedure has been initiated by the expiration of a timer in associated with error-handling procedures.
103	Parameter non-existent or not implemented - passed on (national use)	Indicates the equipment sending this cause has received a message that includes parameters not recognized because the parameters are defined but not implemented by the equipment sending the cause. The parameters were ignored. In addition, if the equipment sending this cause is an intermediate point, this cause indicates the parameters were passed on unchanged.
110	Message with unrecognized parameter discarded	Indicates the equipment sending this cause has discarded a received message that includes a parameter that is not recognized.
111	Protocol error, unspecified	Reports a protocol error event only when no other cause in this class applies. This cause may be displayed if the user failed to dial a 9 or an 8 for an outside line. In addition, this cause may be returned in the event of certain types of restrictions as to number of calls.
122	Precedence level exceeded	Indicates users attempted to make a call with a higher level of precedence than the highest precedence level authorized for their line.
123	Device not preemptable	Indicates one of the following: • The dialed number is non-preemptable. That is, the dialed number registers as busy and has no call waiting, no call forwarding, and no alternate party designations. • The dialed number has a higher precedence level (or priority) than the dialing number and cannot be preempted.
125	Out of bandwidth	Indicates not enough bandwidth was found to connect a call to the destination location.
126	Call split	A Cisco-specific code used by Communications Manager. Indicates a call was terminated during a transfer operation because it was split off and terminated (not part of the final transferred call). This code can help determine which calls were terminated as part of a feature operation.
127	Interworking, unspecified	Indicates an interworking call (usually a call to SW56 service) has ended. May also be seen in the event of a non-specific rejection by a long distance carrier.
129	Precedence out of bandwidth	Indicates not enough bandwidth was found to connect a precedence call to the destination location.
162144 0x40000	Conference full	A Cisco-specific code. Indicates a conference is at full capacity and can accept no new callers.

Termination Code	Description	Explanation
393216 0x60000	Call split	A Cisco-specific code used by Unified Communications Manager. Indicates a call was terminated during a transfer operation because it was split off and terminated (not part of the final transferred call). This code can help determine which calls were terminated as part of a feature operation.
458752 0x70000	Drop any party/drop last party	A Cisco-specific code. Indicates a call was dropped from a conference by the new feature "drop any party/drop last party."

Report_CallJitter

Use this Knowledge Script to categorize calls as having good, acceptable, or poor jitter based on thresholds you set. Calls that do not have a jitter measurement are categorized as having "no data."

You can select only Unified Communications Manager Data Sources for this report. H.323 gateways do not provide jitter measurements.

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source(s)	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Minimum duration	Specify the minimum duration filter for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. The default is 1 second. **Note** Calls that are not completed (i.e., have a duration of 0 seconds) do not generate call jitter data. Therefore, the minimum duration default is 1 second.

Parameter	How to Set It
Group by	Select the delimiter by which you want to group the calls in your report. You can choose from the following sorting options: • **Data Publisher**. Choose this option to sort the report by the Communications Manager Publisher or the Unified Communications Manager primary server. • **Calling Partition** • **Called Partition** • **Calling Location** • **Called Location** • **Outbound Trunk Group** • **Inbound Trunk Group** • **Outbound Gateway** • **Inbound Gateway** • **CallManager Cluster**. This option provides the same sorting results as Data Publisher. This option is maintained in the script to provide backwards compatibility to older versions of AppManager for Call Data Analysis. • **None**. Choose this option to combine all calls into a single group.
Show time details by	Select the time details you want to show for each group of calls. You can choose from the following detail options: • **Hour of Day** • **Day of Week** • **Day of Month** • **None**. If you select None, no time details are shown.
Thresholds	
Threshold - Good-Acceptable jitter	Specify the value below which the call is acceptable and equal to or above which the call is good. The default is 40 ms.
Threshold - Acceptable-Poor jitter	Specify the value below which the call is poor and above which the call is acceptable. The default is 60 ms.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar_Stacked. **Note** To create a chart that indicates the percentage for each category, select **Pie**.
Select output folder	Set parameters for the output folder. The default folder name is CallDataJitter.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Call Jitter.

Parameter	How to Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event if the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_CallJitterLoss

Use this Knowledge Script to categorize the percentage of calls lost due to jitter as being good, acceptable, or poor based on thresholds you set. Only calls from H.323 RADIUS Data Sources can be included in this report because only these Data Sources provide information about discarded packets.

Jitter loss calculations are based on the number of packets received and the number of packets discarded. Discarded packets are those that arrive too early or too late to be stored in the jitter buffer.

Calls that contain no information about received and discarded packets are placed into a "no data" category. In addition, calls that are not completed are not included in the report; they do not contain information about received and discarded packets.

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source(s)	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Minimum duration	Specify the minimum duration filter for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. The default is 1 second. **Note** Calls that are not completed (i.e., have a duration of zero seconds) do not generate data about received and discarded packets. Therefore, the minimum duration default is 1 second.
Group by	Select the delimiter by which you want to group the calls in your report. You can choose from the following sorting options: • **Data Publisher**. Choose this option to sort the report by RADIUS gateway. • **Outbound Gateway** • **Inbound Gateway** • **None**. Choose this option to combine all calls into a single group.

Parameter	How to Set It
Show time details by	Select the time details you want to show for each group of calls. You can choose from the following detail options: • **Hour of Day** • **Day of Week** • **Day of Month** • **None**. If you select None, no time details are shown.
Thresholds	
Threshold - Good-Acceptable percent jitter loss	Specify the percentage below which the jitter loss is acceptable and equal to or above which the jitter loss is good. The default is 0.5%.
Threshold - Acceptable-Poor percent jitter loss	Specify the percentage below which the jitter loss is poor and above which the jitter loss is acceptable. The default is 1.0%.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar_Stacked. **Note** To create a chart that indicates the percentage for each category, select **Pie**.
Select output folder	Set parameters for the output folder. The default folder name is CallDataJitterLoss.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Call Jitter Loss.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event if the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_CallMOS

Use this Knowledge Script to categorize calls as having good, acceptable, or poor MOS or R-value based on thresholds you set.

Calls for which a MOS cannot be calculated are categorized as having "no data." In addition, a MOS is not calculated for calls that are not completed.

MOS is calculated by AppManager (using the E-model) for H.323 RADIUS Data Sources; it is calculated by Cisco (using a Cisco algorithm) for Unified Communications Manager Data Sources.

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source(s)	Select the data for your report by **Type**, **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Minimum duration	Specify the minimum duration filter for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. The default is 1 second. **Note** Calls that are not completed (i.e., have a duration of 0 seconds) do not generate MOS data. Therefore, the minimum duration default is 1 second.

Parameter	How to Set It
Group by	Select the delimiter by which you want to group the calls in your report. You can choose from the following sorting options: • **Data Publisher**. Choose this option to sort the report by RADIUS gateway or Communications Manager Publisher. • **Calling Partition** • **Called Partition** • **Calling Location** • **Called Location** • **Outbound Trunk Group** • **Inbound Trunk Group** • **Outbound Gateway** • **Inbound Gateway** • **CallManager Cluster** • **None**. Choose this option to combine all calls into a single group.
Show time details by	Select the time details you want to show for each group of calls. You can choose from the following detail options: • **Hour of Day** • **Day of Week** • **Day of Month** • **None**. If you select None, no time details are shown.
Thresholds	
Metric	Select whether to analyze call **MOS** or **R-value**. The R-value is calculated from the MOS score. For more information, see "Reviewing Call Quality Metrics for Gateways and Routers" on page 685. If your Data Source is a Communications Manager, do *not* select R-value. Communications Managers provide only a Listening MOS value; an R-value cannot be accurately calculated from a Listening MOS value.
Threshold - Good-Acceptable	Specify the MOS score below which a call is acceptable and equal to or above which a call is good. The default is 4.03.
Threshold - Acceptable-Poor	Specify the MOS score below which a call is poor and above which a call is acceptable. The default is 3.6.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar_Stacked. **Note** To create a chart that indicates the percentage for each category, select **Pie**.
Select output folder	Set parameters for the output folder. The default folder name is CallDataMOS.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.

Parameter	How to Set It
Select properties	Set miscellaneous report properties as desired. The default report name is Call MOS.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is y. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event if the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_CallPacketLoss

Use this Knowledge Script to categorize calls as having a good, acceptable, or poor packet loss percentage based on thresholds you set. Calls that do not have a packet loss measurement are categorized as having "no data."

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source(s)	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Minimum duration	Specify the minimum duration filter for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. The default is 1 second. **Note** Calls that are not completed (i.e., have a duration of 0 seconds) do not generate packet loss data. Therefore, the minimum duration default is 1 second.

Parameter	How to Set It
Group by	Select the delimiter by which you want to group the calls in your report. You can choose from the following sorting options: • **Data Publisher**. Choose this option to sort the report by the entity that generates the data: Communications Manager Publisher, Unified Communications Manager primary server, or RADIUS gateway. • **Calling Partition** (applies to Communications Manager Data Sources) • **Called Partition** (applies to Communications Manager Data Sources) • **Calling Location** (applies to Communications Manager Data Sources) • **Called Location** (applies to Communications Manager Data Sources) • **Outbound Trunk Group** (applies to Communications Manager Data Sources) • **Inbound Trunk Group** (applies to Communications Manager Data Sources) • **Outbound Gateway** (applies to all Data Sources) • **Inbound Gateway** (applies to all Data Sources) • **CallManager Cluster**. This option provides the same sorting results as Data Publisher. This option is maintained in the script to provide backwards compatibility to older versions of AppManager for Call Data Analysis. • **None**. Choose this option to combine all calls into a single group. **Note** If your *Select data source(s)* and *Group by* selections are incompatible (perhaps you selected an H.323 data source and a Communications Manager grouping), the report ignores your *Group by* selection and uses the default selection, which is Data Publisher.
Show time details by	Select the time details you want to show for each group of calls. You can choose from the following detail options: • **Hour of Day** • **Day of Week** • **Day of Month** • **None**. If you select None, no time details are shown.
Thresholds	
Threshold - Good-Acceptable percent packet loss	Specify the value below which the call is acceptable and equal to or above which the call is good. The default is 0.5%.
Threshold - Acceptable-Poor percent packet loss	Specify the value below which the call is poor and above which the call is acceptable. The default is 1.0%.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar_Stacked.
Select output folder	Set parameters for the output folder. The default folder name is CallDataPacketLoss.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.

Parameter	How to Set It
Select properties	Set miscellaneous report properties as desired. The default report name is Call Packet Loss.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event if the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_CallQualityByPhone

Use this Knowledge Script to identify the directory numbers (extensions) experiencing problems with call quality. AppManager calculates call metrics for calls in which the specified directory number originated the call and for calls in which the specified directory number was the destination.

- *Jitter* is an estimate of the statistical variance of the RTP data packet interarrival time, measured in milliseconds and expressed as an unsigned integer. Interarrival jitter is the mean deviation (smoothed absolute value) of the difference in packet spacing at the receiver compared to the sender for a pair of packets.
- *Latency* is the average value of the difference between the time stamp indicted by the senders of the messages and the timestamp of the receivers, measured when the messages are received.
- *MOS* (Mean Opinion Score) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. AppManager uses the MOS Cisco has already calculated using its own algorithm.
- *Packet loss* equals the percentage of data packets lost since the beginning of reception. This number is calculated based on the number of packets expected and the number of packets actually received. The number of packets received includes those that were late or duplicates. Packets that arrive late are not counted as lost; the presence of duplicate packets could result in a negative lost data amount.

You can sort the rows in this report according to its various columns:

- Directory Number
- Duration of Originated Calls
- Average MOS
- Average Jitter
- Average Latency
- Average Packet Loss
- Duration of All Calls
- Success Rate
- Worst MOS
- Worst Jitter
- Worst Latency
- Worst Packet Loss

You can select only Unified Communications Manager Data Sources for this report. H.323 gateways cannot provide the required list of configured directory numbers.

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Minimum duration	Specify the minimum duration filter for calls selected by the script. The default is 0 seconds.
Exclude these failure codes	Specify a list of termination codes (separated by commas) that are not to be considered failures. For more information, see Termination Codes. **Note** Codes 0, 16, 31, and 127 are automatically excluded. They are normal termination codes. However, these codes may appear in events if the other side of the call has a failure code that has not been excluded.
Search Criteria	
Note for entering search criteria: If you specify only the wildcard (*) for a field (such as calling number), AppManager matches *only* those calls that have a value for that field. Calls for which that field has no value (i.e., is NULL) will not be matched. For example, if you specify * in the *Calling partition name* parameter, the search matches only those calls that have some partition name configured. To match all calls (including calls that have no value for the selected field), leave the search criteria parameter blank.	
Directory number	Specify the directory numbers for which you want to identify call quality problems.
Device name	Specify the device names for which you want to identify call quality problems.
Device IP address	Specify the IP address of the devices you want to find. Use one of the following formats: • Single dotted-decimal IP address, such as 10.41.2.31 • Dotted-decimal IP address that includes a wildcard, such as 10.41.*.*, which would search for all IP addresses in the range of 10.41.0.0 to 10.41.255.255. • Range of dotted-decimal IP addresses separated by a hyphen, such as 10.41.2.31-10.41.2.41. The first address indicates the beginning of the range; the second IP address marks the end of the range.
Device location name	Specify the names of the device locations for which you want to identify call quality problems. Use the location configured on the Unified Communications Manager.
Partition name	Specify the partition names for which you want to identify call quality problems.
Report Settings	
Order rows by?	Select the column by which you want to sort the rows in the report.
MOS type?	Select whether to display **Average** or **Minimum** MOS in your report. • Average MOS is the running average of scores observed since the beginning of a call. • Minimum MOS is the minimum score observed since the beginning of a call, and represents the worst-sounding eight-second interval.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.

Parameter	How to Set It
Select output folder	Set parameters for the output folder. The default folder name is CallQualityByPhone.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Call Quality By Phone.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_CallSuccessRate

Use this Knowledge Script to determine the success rate of calls recorded with the selected Data Source. A successful call is determined by the call's disconnect cause code.

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source(s)	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.

Parameter	How to Set It
Group by	Select the delimiter by which you want to group the calls in your report. You can choose from the following sorting options: • **Data Publisher**. Choose this option to sort the report by the entity that generates the data: Communications Manager Publisher, Unified Communications Manager primary server, or RADIUS gateway. • **Calling Partition** (applies to Communications Manager Data Sources) • **Called Partition** (applies to Communications Manager Data Sources) • **Calling Location** (applies to Communications Manager Data Sources) • **Called Location** (applies to Communications Manager Data Sources) • **Outbound Trunk Group** (applies to Communications Manager Data Sources) • **Inbound Trunk Group** (applies to Communications Manager Data Sources) • **Outbound Gateway** (applies to all Data Sources) • **Inbound Gateway** (applies to all Data Sources) • **CallManager Cluster**. This option provides the same sorting results as Data Publisher. This option is maintained in the script to provide backwards compatibility to older versions of AppManager for Call Data Analysis. • None. Choose this option to combine all calls into a single group. **Note** If your *Select data source(s)* and *Group by* selections are incompatible (perhaps you selected an H.323 data source and a Communications Manager grouping), the report ignores your *Group by* selection and uses the default selection, which is Data Publisher.
Show time details by	Select the time details you want to show for each group of calls. You can choose from the following detail options: • **Hour of Day** • **Day of Week** • **Day of Month** • **None**. If you select None, no time details are shown.
Exclude these failure codes	Specify a list of termination codes (separated by commas) that are not to be considered failures. For more information, see Termination Codes. **Note** Codes 0, 16, 31, and 127 are automatically excluded. They are normal termination codes. However, these codes may appear in events if the other side of the call has a failure code that has not been excluded.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CallDataSuccessRate.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.

Parameter	How to Set It
Select properties	Set miscellaneous report properties as desired. The default report name is Call Success Rate.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_CallTraffic

Use this Knowledge Script to summarize call traffic by call type.

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source(s)	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Minimum duration	Specify the minimum duration filter for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. The default is 0 seconds.

Parameter	How to Set It
Group by	Select the delimiter by which you want to group the calls in your report. You can choose from the following sorting options: • **Data Publisher**. Choose this option to sort the report by the entity that generates the data: Communications Manager Publisher, Unified Communications Manager primary server, or RADIUS gateway. • **Calling Partition** (applies to Communications Manager Data Sources) • **Called Partition** (applies to Communications Manager Data Sources) • **Calling Location** (applies to Communications Manager Data Sources) • **Called Location** (applies to Communications Manager Data Sources) • **Outbound Trunk Group** (applies to Communications Manager Data Sources) • **Inbound Trunk Group** (applies to Communications Manager Data Sources) • **Outbound Gateway** (applies to all Data Sources) • **Inbound Gateway** (applies to all Data Sources) • **CallManager Cluster**. This option provides the same sorting results as Data Publisher. This option is maintained in the script to provide backwards compatibility to older versions of AppManager for Call Data Analysis. • **None**. Choose this option to combine all calls into a single group. **Note** If your *Select data source(s)* and *Group by* selections are incompatible (perhaps you selected an H.323 data source and a Communications Manager grouping), the report ignores your *Group by* selection and uses the default selection, which is Data Publisher.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.

Show duration in Erlangs or seconds?	Select whether to display call duration in **Erlangs** or **Seconds**. The default is Erlangs.
	Also known as a traffic unit, an Erlang is a measurement of traffic load during the busy hour, and is based on having 3600 seconds (60 minutes or one hour) of calls on the same circuit, trunk, or port. (In other words, one circuit is busy for one hour regardless of the number of calls or the average length of calls). For example, if a call center received 30 six-minutes calls in the busy hour, it received 180 call minutes, or three Erlangs. If a call center received 100 calls that averaged 36 seconds in the busy hour, it received 3600 call seconds or one Erlang.
	You can use the following formula to calculate an Erlang value:
	`Traffic in Erlangs =`
	`(Number of calls in the busy hour) * (AHT seconds)/3600`

Select chart style	Define the graphic properties for the charts in your report. The default style is Bar_Stacked. **Note** To create a chart that indicates the percentage of each type of call, select **Pie**.
Select output folder	Set parameters for the output folder. The default folder name is CallDataTraffic.

Parameter	How to Set It
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Call Traffic.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_CallVolume

Use this Knowledge Script to summarize the number and duration of calls recorded with the selected Data Source.

In this report, calls that have an originating gateway and a terminating gateway that are different are associated with the originating gateway. For a clearer view of incoming and outgoing calls on a per-gateway basis, use the Report_TrunkGroupByHour report.

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source(s)	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Minimum duration	Specify the minimum duration filter for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. The default is 0 seconds.

Parameter	How to Set It
Group by	Select the delimiter by which you want to group the calls in your report. You can choose from the following sorting options: • **Data Publisher**. Choose this option to sort the report by the entity that generates the data: Communications Manager Publisher, Unified Communications Manager primary server, or RADIUS gateway. • **Calling Partition** (applies to Communications Manager Data Sources) • **Called Partition** (applies to Communications Manager Data Sources) • **Calling Location** (applies to Communications Manager Data Sources) • **Called Location** (applies to Communications ManagerData Sources) • **Outbound Trunk Group** (applies to Communications Manager Data Sources) • **Inbound Trunk Group** (applies to Communications Manager Data Sources) • **Outbound Gateway** (applies to all Data Sources) • **Inbound Gateway** (applies to all Data Sources) • **CallManager Cluster**. This option provides the same sorting results as Data Publisher. This option is maintained in the script to provide backwards compatibility to older versions of AppManager for Call Data Analysis. • **None**. Choose this option to combine all calls into a single group. **Note** If your *Select data source(s)* and *Group by* selections are incompatible (for instance, if you selected an H.323 data source and a Communications Manager grouping), the report ignores your *Group by* selection and uses the default selection, which is Data Publisher.
Show time details by	Select the time details you want to show for each group of calls. Choose from the following detail options: • **Hour of Day** • **Day of Week** • **Day of Month** • **None**. If you select None, no time details are shown.
Group time details based on	Select the way in which you want to group the time details for calls. Choose one of the following: • **Start time** - to group entire calls by the time periods in which the calls start. For example, you choose to group calls by Hour of Day. Five calls begin during the 12:00 hour. Regardless of the duration of the calls, the report will show five calls during the 12:00 hour. • **Call duration** - to split calls into multiple groups based on the duration of the calls. For example, you choose to group calls by Hour of Day. Five calls begin during the 12:00 hour. Three of the calls complete during the 12:00 hour, two calls complete during the 1:00 hour, and one call that began at 11:45 completes during the 12:00 hour. The report will show four calls during the 12:00 hour and two calls during the 1:00 hour.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.

Parameter	How to Set It
Units for chart	Select the unit of measurement that should appear on the Y axis of the chart: **Duration** or **Number Of Calls**. The default is Number of Calls. If you select Duration, the duration unit measurement is determined by the value you select in the *Show duration in Erlangs or seconds?* parameter.

Show duration in Erlangs or seconds?	Select whether you want the duration measurement to display in Erlangs or seconds. The default is Erlangs.
	Also known as a traffic unit, an Erlang is a measurement of traffic load during the busy hour, and is based on having 3600 seconds (60 minutes or one hour) of calls on the same circuit, trunk, or port. (In other words, one circuit is busy for one hour regardless of the number of calls or the average length of calls). For example, if a call center received 30 six-minutes calls in the busy hour, it received 180 call minutes, or three Erlangs. If a call center received 100 calls that averaged 36 seconds in the busy hour, it received 3600 call seconds or one Erlang.
	You can use the following formula to calculate an Erlang value:
	`Traffic in Erlangs =`
	`(Number of calls in the busy hour) * (AHT seconds)/3600`

Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CallDataVolume.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Call Volume.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_CCME_StatsByEPhone

Use this Knowledge Script to summarize the call statistics for Cisco Communications Manager Express phones (ephones) based on configuration information retrieved by the CCME_GetConfig Knowledge Script. You must run GetConfig and the Data Collection job before you can run StatsByEPhone.

This report can summarize the following call statistics:

- Communications Manager Express
- Total Duration
- Duration of Originated Calls
- Completed Calls
- Completion Rate
- Total Calls
- Originated Calls
- Failed Calls
- Success Rate

You can sort the rows in this report according to its various columns:

- Directory Number
- Duration of Originated Calls
- Completion Rate
- Duration of All Calls
- Number of Originated Calls
- Success Rate

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**. You may select only one H.323 RADIUS data source.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Minimum duration	Specify the minimum duration filter for calls selected by the script. The default is 0 seconds.

Parameter	How to Set It
Exclude these failure codes	Type a list of termination codes (separated by commas) that are not to be considered failures. For more information, see Termination Codes. **Note** Codes 0, 16, 31, and 127 are automatically excluded. They are normal termination codes. However, these codes may appear in events if the other side of the call has a failure code that has not been excluded.
Search Criteria	
Note for entering search criteria: If you specify only the wildcard (*) for a field (such as calling number), AppManager matches *only* those calls that have a value for that field. Calls for which that field has no value (i.e., is NULL) will not be matched. For example, if you specify * in the *Calling partition name* parameter, the search matches only those calls that have some partition name configured. To match all calls (including calls that have no value for the selected field), leave the search criteria parameter blank.	
Gateway name	Specify the name of the Communications Manager Express gateway for which you want to gather call statistics. Leave this field blank to gather statistics for *all* Communications Manager Express gateways.
Directory number	Specify the directory number for which you want to gather call statistics.
Device name	Specify the name of the device for which you want to gather call statistics.
Device IP address	Specify the IP addresses of the devices you want to find. Use one of the following formats: • Single dotted-decimal IP address, such as 10.41.2.31 • Dotted-decimal IP address that includes a wildcard, such as 10.41.*.*, which would search for all IP addresses in the range of 10.41.0.0 to 10.41.255.255. • Range of dotted-decimal IP addresses separated by a hyphen, such as 10.41.2.31-10.41.2.41. The first address indicates the beginning of the range; the second IP address marks the end of the range.
Report Settings	
Order rows by?	Select the column by which you want to sort the rows in the report. The default is DirectoryNumber.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is CCME_StatsByEPhone.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CME Call Statistics By EPhone.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.

Parameter	How to Set It
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_CCME_Summary

Use this Knowledge Script to summarize the following call statistics for Cisco Communications Manager Express gateways:

- Number of calls
- Completed calls
- Abandoned calls
- Completion rate
- Total duration
- Failed calls
- Success rate

By default, these statistics are broken down by incoming vs. outgoing calls from and to Communications Manager Express phones — details are shown for outgoing, incoming, and local Communications Manager Express calls.

In addition, you can choose to break down the statistics by Communications Manager Express calls to and from the PSTN vs. calls to and from the IP network. If you choose this option, details are shown for calls outgoing to the PSTN, outgoing to the IP, incoming from the PSTN, and incoming from the IP, and for local Communications Manager Express calls.

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**. You may select only one H.323 RADIUS data source.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Gateway name	Specify the name of the Communications Manager Express gateway for which you want to gather call statistics. Leave this field blank to gather statistics for *all* Communications Manager Express gateways.
Minimum duration	Specify the minimum duration filter for calls selected by the report. The default is 0 seconds.

Parameter	How to Set It
Exclude these failure codes	Type a list of termination codes (separated by commas) that are not to be considered failures. For more information, see Termination Codes. **Note** Codes 0, 16, 31, and 127 are automatically excluded. They are normal termination codes. However, these codes may appear in events if the other side of the call has a failure code that has not been excluded.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of call statistics in the report. The default is y.
Include chart?	Set to **y** to include a chart of call statistics in the report. The default is y. If you choose to include a chart, use the *Select call statistic for chart* parameter to select the statistic you want to display in the chart.
Show breakdown of PSTN calls vs. IP calls?	Set to **y** to include a breakdown of statistics by Communications Manager Express calls to/from the PSTN vs. calls to/from the IP network. If you choose this option, details are shown for calls outgoing to the PSTN, outgoing to the IP, incoming from the PSTN, and incoming from the IP, and for local Communications Manager Express calls. The default is n.
Select call statistic for chart	Select the call statistic you want to display, per gateway, in a chart in the report. You can choose from: • **Number of Calls** (default) • **Duration** • **Success Rate** • **Completion Rate**

Show duration in Erlangs or seconds?	Select whether to display call duration in **Erlangs** or **Seconds**. The default is Erlangs.
	Also known as a traffic unit, an Erlang is a measurement of traffic load during the busy hour, and is based on having 3600 seconds (60 minutes or one hour) of calls on the same circuit, trunk, or port. (In other words, one circuit is busy for one hour regardless of the number of calls or the average length of calls). For example, if a call center received 30 six-minutes calls in the busy hour, it received 180 call minutes, or three Erlangs. If a call center received 100 calls that averaged 36 seconds in the busy hour, it received 3600 call seconds or one Erlang.
	You can use the following formula to calculate an Erlang value:
	`Traffic in Erlangs =`
	`(Number of calls in the busy hour) * (AHT seconds)/3600`

Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CCME_CallSummary.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CME Call Summary.

Parameter	How to Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_FrequentlyCalledNumbers

Use this Knowledge Script to display any destination phone numbers called frequently during a specified time range. The report contains three columns: Called Number, Total Calls, and Total Duration.

Identifying Toll Fraud

The concept of toll fraud encompasses two separate but related security problems: frequently called numbers and the inappropriate use of long-distance capabilities, such as overly long calls to foreign countries or 900 numbers.

You can use the Report_FrequentlyCalledNumbers Knowledge Script to discover whether any particular phone number is being called more often than seems reasonable. Perhaps a once-a-month call to a European client is acceptable, but ten calls in one week indicates a problem.

The Report_FrequentlyCalledNumbers Knowledge Script creates a table that identifies the destination number, the number of calls made to the destination number, and the total duration of all calls made to the destination number. You set the threshold for "too many" calls — the report will display data for every destination phone number that received more calls than that threshold. Then use the Report_CallDetail_CiscoCallMgr Knowledge Script to identify the originating phone number of all calls made to the phone number in question.

The CallDetail_CiscoCallMgr Knowledge Script can also help your efforts to identify overly long calls. For instance, while making rounds, a courier went from office to office, picked up a phone in a public area, dialed a premium number, and then left, leaving the call active. The companies were billed for several hours of charges to the premium number.

With the Report_CallDetail_CiscoCallMgr Knowledge Script, you can create a report that looks for trends in overly long calls. Set the *Maximum duration* parameter to the maximum length of an acceptable call. Acceptable durations will vary by company, but for this scenario, let us say ten minutes. The report will present a list of calls that exceed the ten-minute limit.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Search Criteria	

Parameter	How to Set It
Called number pattern	Specify the phone number pattern you want to find. The pattern can include the * wildcard. For example, to search for external calls, type 9*. Leave this parameter blank to include all calls in the report, as long as all other criteria are satisfied.
Minimum duration of each call	Specify the minimum duration filter for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. Accept the default of 0 to indicate no limit.
Minimum number of calls	Specify the minimum number of times a number must be called before it can be included in your report. For example, if you type 5, your report will include only those numbers called five or more times. The default is 2 calls.
Report Settings	
Maximum number of rows to return	Specify the maximum number of rows to include in the table in the report. The default is 1000 rows. **Note** No matter how many rows you choose to include in the report, the report will indicate how many rows actually met your search criteria. This number may, and probably will, exceed the number of rows you choose to return.
Order rows by?	Select the delimiter by which you want to sort the calls in your report. You can choose from the following sorting options: • **Total Calls** (default) • **Total Duration** • **Called Number**

Show duration in Erlangs or seconds?	Select whether to display call duration in **Erlangs** or **Seconds**. The default is Seconds.
	Also known as a traffic unit, an Erlang is a measurement of traffic load during the busy hour, and is based on having 3600 seconds (60 minutes or one hour) of calls on the same circuit, trunk, or port. (In other words, one circuit is busy for one hour regardless of the number of calls or the average length of calls). For example, if a call center received 30 six-minutes calls in the busy hour, it received 180 call minutes, or three Erlangs. If a call center received 100 calls that averaged 36 seconds in the busy hour, it received 3600 call seconds or one Erlang.
	You can use the following formula to calculate an Erlang value:
	`Traffic in Erlangs =`
	`(Number of calls in the busy hour) * (AHT seconds)/3600`

Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is FrequentlyCalledNumbers.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Frequently Called Numbers.

Parameter	How to Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event if the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_GatewayDialPeers

Use this Knowledge Script to summarize call statistics for the POTS (Plain Old Telephone System) and VoIP dial peers of the gateways included in the report. By default, these statistics include total calls, total duration, failed calls, and success rate. You can choose to include call quality statistics for VoIP dial peers.

A dial peer is the association of a dialed sequence of numbers with a device in a telephone network. In a POTS network, a dial peer maps to a specific voice port on a local router or gateway. In a VoIP network, a dial peer maps to a remote network device, such as a router, a gateway, or a Cisco Unified Communications Manager. There is a one-to-one correspondence between a dial peer and a call leg.

A call leg is a component of the accounting records generated by a Cisco H.323 gateway. A call leg represents a logical connection between the gateway and a telephony or IP endpoint. Each call processed through a gateway consists of one or more call legs.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**. You can select only one H.323 RADIUS Data Source.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Gateway name	Indicate the name of the gateway for which you want to summarize call statistics. Leave this field blank to summarize statistics for *all* gateways associated with the Data Source
Direction of calls	Select the direction of the calls for which you want to summarize statistics. Choose from **Inbound Only**, **Outbound Only**, or **Inbound and Outbound**. The default is Inbound and Outbound.
Type of dial peer	Select the dial peer for which you want to summarize call statistics. Choose from **POTS Only**, **VoIP Only**, or **POTS and VoIP**. The default is POTS and VoIP.
Minimum duration	Specify the minimum duration filter for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. The default is 0 seconds.

Parameter	How to Set It
Exclude these failure codes	Specify a list of termination codes (separated by commas) you do not want to include in the report. In other words, any call that terminates with one of the listed codes will not be included in the report. For more information, see Termination Codes. **Note** Codes 0, 16, 31, and 127 are automatically excluded. They are normal termination codes. However, these codes may appear in events if the other side of the call has a failure code that has not been excluded.
Report Settings	
Include quality metrics?	Select whether to include call quality metrics in the report. You can choose from **Metrics with a MOS**, **Metrics with an R-value**, or **No Metrics**. For more information, see "Reviewing Call Quality Metrics for Gateways and Routers" on page 685.

Show duration in Erlangs or seconds?	Select whether to display call duration in **Erlangs** or **Seconds**. The default is Seconds.
	Also known as a traffic unit, an Erlang is a measurement of traffic load during the busy hour, and is based on having 3600 seconds (60 minutes or one hour) of calls on the same circuit, trunk, or port. (In other words, one circuit is busy for one hour regardless of the number of calls or the average length of calls). For example, if a call center received 30 six-minutes calls in the busy hour, it received 180 call minutes, or three Erlangs. If a call center received 100 calls that averaged 36 seconds in the busy hour, it received 3600 call seconds or one Erlang.
	You can use the following formula to calculate an Erlang value:
	`Traffic in Erlangs =`
	`(Number of calls in the busy hour) * (AHT seconds)/3600`

Order rows by?	Select the delimiter by which you want to sort the calls in your report. You can choose from the following sorting options: • **Dial Peer** (default) • **Number of Calls** • **Duration of Calls** • **Success Rate**
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is GatewayDialPeers.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco Voice Gateway Dial Peers.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event if the report is successfully generated. The default is y.

Parameter	How to Set It
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_TrunkGroupByHour

Use this Knowledge Script to display the trunk group or gateway volume by hour for the selected Cisco Unified Communications Manager clusters or to display the gateway, trunk group, or interface volume for the selected H.323 RADIUS Data Source. The report includes a breakdown of calls that are inbound, outbound, or both (tandem).

A Communications Manager trunk group points to a series of devices (gateways or intercluster trunks to remote Communications Managers) through which calls are to be routed.

An H.323 gateway trunk group consists of a set of interfaces on the gateway configured to belong to the trunk group.

Note
Unlike other modules, for the Call Data Analysis module, the Report agent pulls data from the Data Warehouse rather than from the AppManager repository. The Report agent uses Windows authentication to access the Data Warehouse.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source(s)	Select the data for your report by **Data Source Type**, **View Name**, **Data Warehouse**, and **Data Source**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Show results by	Select whether to show results for **Trunk Groups**, **Gateways**, or **Interfaces**. The default is Trunk Groups. The Interfaces option is valid only for H.323 RADIUS Data Sources.
Gateway name	Use this parameter to specify which gateways to include in the report. Specify the name of the gateway you want to include in the report. To include multiple gateways, use the * as a wildcard character. For example, type RAL* to include the gateways named RAL001, RAL003, and RAL010. Leave this parameter blank to include all gateways. This parameter is valid only for H.323 RADIUS Data Sources.
Minimum duration	Specify the minimum duration filter for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. The default is 0 seconds.
Report Settings	

Parameter	How to Set It
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Units for chart and peak hour calculation	Select the unit of measurement that should appear on the Y axis of the chart: **Duration** or **Number Of Calls**. The default is Number of Calls. If you select Duration, the duration unit measurement is determined by the value you select in the *Show duration in Erlangs or seconds?* parameter.

Show duration in Erlangs or seconds?	Select whether to display call duration in **Erlangs** or **Seconds**. The default is Erlangs.
	Also known as a traffic unit, an Erlang is a measurement of traffic load during the busy hour, and is based on having 3600 seconds (60 minutes or one hour) of calls on the same circuit, trunk, or port. (In other words, one circuit is busy for one hour regardless of the number of calls or the average length of calls). For example, if a call center received 30 six-minutes calls in the busy hour, it received 180 call minutes, or three Erlangs. If a call center received 100 calls that averaged 36 seconds in the busy hour, it received 3600 call seconds or one Erlang.
	You can use the following formula to calculate an Erlang value:
	`Traffic in Erlangs =`
	`(Number of calls in the busy hour) * (AHT seconds)/3600`

Select chart style	Define the graphic properties for the charts in your report. The default style is Bar_Stacked.
Select output folder	Set parameters for the output folder. The default folder name is TrunkGroupByHour.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Trunk Group By Hour.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_UnusedPhones

Use this Knowledge Script to create a list of unused phones. This script bases the report on the list of phones configured on Cisco Unified Communications Manager or Unified Communications Manager Express. It looks at the phones configured at the time of the most recent successful data collection, and then, using the criteria you set in the parameters, creates a list of phones that have been unused for *n* days.

When running this script, keep in mind how far back the data goes, including the initial data load. If you specify an initial data load of seven days, and then run this script, any phone whose last call was at least eight days ago will show up on the report as having no calls — in other words, as unused.

You can select Communications Managers or H.323 gateways as Data Sources for this report. Before using this report to identify unused Communications Manager Express phones (based on the H.323 gateways you select), run the CCME_GetConfig Knowledge Script, which provides meaningful data for all Communications Manager Express phones.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data source	Select the data for your report by **View Name**, **Data Warehouse**, or **Data Source**. To work with Communications Manager Express phones, select **H.323 Gateways**.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Gateway name	Use this parameter *only* if you selected **H.323 Gateways** as a data source. Specify the name of the Communications Manager Express gateway for which you want to find unused phones. Alternatively, type a partial name and the * wildcard to indicate Communications Manager Express names that match a pattern. Leave this field blank to gather statistics for *all* Communications Manager Express gateways known by the data source.
Minimum days since last call	Specify the minimum unused days filter for calls selected by the script. Phones unused for less than the minimum will not be included in the report, even if all other criteria are satisfied. Type 0 to include all unused phones in the report.
Minimum duration when looking for calls	Specify the minimum duration filter for calls selected by the script. Calls with a duration of less than the minimum will not be included in the report, even if all other criteria are satisfied. The default is 0 seconds.

Parameter	How to Set It
Direction of calls	Specify the direction filter for calls selected by the script. You can choose to include calls that are **Outbound Only**, **Inbound Only**, or both **Inbound and Outbound**.
Report Settings	
Order rows by?	Select the criterion by which you want to sort the rows in the report: • **Most Recently Used**. In order by date from the most recently used phone to the least recently used phone. • **Least Recently Used**. In order by date from the least recently used phone to the most recently used phone. All phones used on any given day are sorted by directory number. For example, the report may show 10 phones used on April 4, 7 phones used on April 3, and 12 phones used on April 2. April 4th's 10 phones are sorted by directory number, as are the phones for April 3 and April 2.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is UnusedPhones.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Unused Phones.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

UpdateSecurity

Use this Knowledge Script to update the user IDs and passwords associated with a Data Source. This script raises an event when an update succeeds or fails, or when the Data Mart server is inaccessible.

Resource Objects

Call Data CallManager object

Call Data H.323 RADIUS object

Call Data CiscoCM object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Update data source security?	Set to **Yes** if you want to update the username and password for a Communications Manager Data Source. The default is unselected. **Note** This parameter is not applicable for H.323 RADIUS Data Sources, for which no security information is required.
SQL username	Type the SQL username that provides access to the Communications Manager Data Source computer. Leave this field blank to use Windows authentication. **Note** This parameter is not applicable for H.323 RADIUS Data Sources, for which no security information is required.
SQL password	Type the SQL password associated with the SQL username. If you leave the *SQL username* field blank, the script ignores this parameter. **Note** This parameter is not applicable for H.323 RADIUS Data Sources, for which no security information is required.
Update data mart security?	Select **Yes** if you want to update the username and password for the Data Mart. The default is unselected.
SQL username	Type the SQL username that provides access to the Data Mart computer. Leave this field blank to use windows authentication.
SQL password	Type the SQL password associated with the SQL username. If you leave the *SQL username* field blank, the script ignores this parameter.
Update Data Warehouse access?	Select **Yes** if you want to update the username and password for the Data Warehouse. The default is unselected. **Note** The username and passwords for the Data Warehouse access are used for accessing both the local NetIQ agent (`netiqmc` service) AND the SQL Server agent service running on the Data Mart computer.
SQL username	Type the SQL username that provides access to the Data Warehouse computer. Leave this field blank to use Windows authentication.
SQL password	Type the SQL password associated with the SQL username. If you leave the *SQL username* parameter blank, the script ignores this parameter.

Parameter	How to Set It
Event Notification	
Raise event if update succeeds?	Select **Yes** to raise an event when the update is successful. The default is Yes.
Event severity when update succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event when the update is successful. The default is 25.
Event severity when data mart server is inaccessible	Set the severity level, from 1 to 40, to indicate the importance of the event when the Data Mart computer is inaccessible. The default is 10.
Event severity when update fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the update fails. The default is 5.

Chapter 17
CallSetup Knowledge Scripts

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press F1.

Knowledge Script	What It Does
H.323_CallSetup_Direct	Sets up a VoIP call directly between NetIQ endpoints over H.323 without the use of a gatekeeper or a gateway.
H.323_CallSetup_Gatekeeper	Sets up a VoIP call between NetIQ endpoints over H.323 using a gatekeeper.
H.323_CallSetup_Gateway	Sets up a VoIP call between NetIQ endpoints over H.323 using a gateway.
H.323_Listen	Causes the NetIQ endpoint to begin listening for H.323 communications on a given port.
H.323_Registration	Registers a NetIQ endpoint with a gatekeeper over H.323.
H.323_UpdateAlias	Updates the alias name of the H.323 resource in the repository.
Report_H.323Configuration	Displays the Call Setup H.323 configuration for the selected computers.
Report_H.323ResponseAvailMatrix	Displays the average response time and availability between talkers and listeners.
Report_H.323ResponseTimeDetail	Displays the average response time by minute.
Report_SIPConfiguration	Displays the Call Setup SIP configuration for the selected computers.
Report_SIPResponseAvailMatrix	Displays the average response time and availability between talkers and listeners.
Report_SIPResponseTimeDetail	Displays the average response time by minute.
SIP_CallSetup_Direct	Performs all of the steps associated with setting up a VoIP call using SIP directly between two endpoints.
SIP_CallSetup_Server	Performs all of the steps associated with setting up a VoIP call using a SIP server.
SIP_Listen	Causes the NetIQ endpoint to begin listening for SIP communications on a given port.
SIP_Registration	Performs basic registration with the server and checks for response time, a valid response, and a successful return code.
SIP_UpdateAlias	Updates the alias name of the SIP resource in the repository.

H.323_CallSetup_Direct

Use this Knowledge Script to set up a VoIP call between NetIQ endpoints (one listener and one talker) over H.323 without the use of a gatekeeper or a gateway.

A direct call setup test tears down the call. The tear down is not included in the response time measurement. This script raises an event if response time exceeds the threshold that you set.

You can set up an H.323 call across a LAN to ensure that an H.323 device, such as NetMeeting, can make direct calls. This "loop back" monitoring job helps you verify proper installation and configuration of H.323 agent devices. In addition, you can determine the response time, which indicates LAN performance, for H.323 call setup between client devices.

Prerequisite

Run the H.323_Listen script without specifying gatekeeper information on the Values tab. You cannot initiate a CallSetup Knowledge Script job unless you first run the Listen job.

Resource Object

H.323 object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How to Set It
Collect data?	Select **y** to collect data about response time for reports and graphs. The default is y.
Select listener(s)	Select the names of the computers that you want to act as listeners.
Threshold - Maximum response time	Specify the maximum amount of response time that can occur before an event is raised. The default is 500 milliseconds.
Event severity when response time exceeds the threshold	Set the event severity level, from 1 to 40, to reflect the importance of an event in which response time exceeds the threshold. The default is 15.
Event severity when call setup fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the call setup test fails. The default is 5.
Listening port number	Enter the port number of the listening endpoint. This port number must match that of the listening port you specified in the H.323_Listen script. The default port number is 1720.
Use H.245 tunneling?	Select **y** to enable H.245 message encapsulation. The default is n.

H.323_CallSetup_Gatekeeper

Use this Knowledge Script to set up a VoIP call between NetIQ endpoints (one listener and one talker) over H.323 using a gatekeeper. A gatekeeper call is one in which the gatekeeper confirms the availability of the listener before allowing the talker to complete a call.

A gatekeeper call setup test tears down the call. The tear down is not included in the response time measurement. This script raises an event if response time exceeds the threshold that you set.

You can set up an H.323 call through a router gatekeeper to determine the response time, which indicates performance, for H.323 call setup across a WAN or to the PSTN (Public Switched Telephone Network).

Tip
Run the H.323_Registration script on the agent computer to monitor the gatekeeper's availability by registering and deregistering the agent computer with the gatekeeper.

Prerequisite

Run the H.323_Listen script and specify *all* of the gatekeeper parameters on the Values tab. The Listen script prepares the listener endpoint for listening. You cannot initiate a CallSetupKnowledge Script job unless you first run the Listen job.

Resource Object

H. 323 object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Collect data?	Select **y** to collect data about response time for reports and graphs. The default is y.
Select listener(s)	Select the names of the computers that you want to act as listeners.
Threshold - Maximum response time	Specify the maximum amount of response time that can occur before an event is raised. The default is 500 milliseconds.
Event severity when response time exceeds the threshold	Set the event severity level, from 1 to 40, to reflect the importance of an event in which response time exceeds the threshold. The default is 15.
Event severity when call setup fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the call setup test fails. The default is 5.
Name or IP address of gatekeeper	Enter the name or IP address of the gatekeeper. If you enter an incorrect IP address or leave the field blank, then this job will fail.

Parameter	How To Set It
Port to communicate with gatekeeper	Enter the port on the gatekeeper with which the signaling (talker) and listening ports will communicate in order to communicate with the gatekeeper. If you entered a name or IP address in *Name or IP address of gatekeeper*, then you *must* provide the port number. If you enter an incorrect port number or leave the field blank, then this job will fail. The default port number is 1719.
Password for use of gatekeeper	Enter the password, if any, associated with the gatekeeper. If you entered a name or IP address in *Name or IP address of gatekeeper*, then you *must* provide the applicable password. If you enter an incorrect password or leave the field blank, then this job will fail.
Use H.245 tunneling?	Select **y** to enable H.245 message encapsulation. The default is n.

H.323_CallSetup_Gateway

Use this Knowledge Script to set up a VoIP call between NetIQ endpoints (one listener and one talker) over H.323 using a gateway. A gateway call is one in which the talker funnels a call through a gateway, which determines the route of the call and availability of the listener. The gateway sends the call on to the listener.

A gateway call setup test tears down the call. The tear down is not included in the response time measurement.This script raises an event when response time exceeds the threshold that you set.

Some gateways may not be able to handle call setup tests for multiple calls or multiple listeners. For example, your test may fail if you attempt to set up a test with two listeners (from talker A to listeners B and C). In this case, run two separate call setup tests for the two calls: one from talker A to listener B, and another from talker A to listener C.

You can set up an H.323 call through a router gateway to determine the response time, which indicates performance, for H.323 call setup across a WAN or to the PSTN (Public Switched Telephone Network).

You can set up an H.323 call through Cisco Unified Communications Manager to ensure that Cisco soft phones can make calls. This "loop back" monitoring job helps you determine the response time, which indicates performance, for H.323 call setup through Communications Manager.

Notes

- Cisco Unified Communications Manager provides H.323 gateway services for soft phones because the phones use H.323, not SCCP, for call setup. You must manually configure all soft phones on a Communications Manager.
- If the name of the agent phone in AppManager is not the same as the "Device Name" in Communications Manager, run H.323_UpdateAlias. In the *New alias name* parameter, enter the same description that is used for the Communications Manager phone configuration "Device Name."
- Because Communications Manager is not a gatekeeper for H.323 devices, do not run H.323_CallSetup_Gatekeeper or H.323_Registration against a Communications Manager server.

Prerequisites

- Configure the gateway to associate the hostname of the endpoint computer with an H.323 alias, an arbitrary value that you determine.
- Run the H.323_UpdateAlias script to pull the configured alias information into AppManager.
- Run the H.323_Listen script without specifying any gatekeeper information on the Values tab. The Listen script prepares the listener endpoint for listening. You cannot initiate a CallSetup Knowledge Script job unless you first run a Listen job.

Resource Object

H. 323 object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Collect data?	Select **y** to collect data about response time for reports and graphs. The default is y.
Select listener(s)	Select the names of the computers that you want to act as listeners. **Note** Some gateways may not be able to handle call setup tests for multiple listeners. For example, your test may fail if you select two computers for this parameter. In this case, simply run this script twice — once for the first computer and then again for the second.
Threshold - Maximum response time	Specify the maximum amount of response time that can occur before an event is raised. The default is 500 milliseconds.
Event severity when response time exceeds the threshold	Set the event severity level, from 1 to 40, to reflect the importance of an event in which response time exceeds the threshold. The default is 15.
Event severity when call setup fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the call setup test fails. The default is 5.
Name or IP address of gateway	Enter the name or IP address of the gatekeeper. If you enter an incorrect IP address or leave the field blank, then this job will fail.
Port to communicate with gateway	Enter the port on the gatekeeper with which the signaling (talker) and listening ports will communicate in order to communicate with the gatekeeper. If you enter an incorrect port number or leave the field blank, then this job will fail. The default port number is 1720.
Use H.245 tunneling?	Select **y** to enable H.245 message encapsulation. The default is n.

H.323_Listen

Use this Knowledge Script to cause the NetIQ endpoint to begin listening for H.323 communications on a given port. This script restarts the listening process on any agent computer whose endpoint goes down for any reason. It does not check against running multiple listening jobs on the same computer for the same alias and port — that is the job of the managed object.

The listening test will perform registration if the gatekeeper is specified in the script parameters. It is not necessary to perform both the registration test and the listening test. However, you must run the listen test before running any of the call setup tests.

Resource Object

H.323 object

Default Schedule

By default, this script runs on an asynchronous schedule.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Event severity when listening job fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the listening job fails. The default is 5.
Listening port number	Enter the number of the listening port. The default is 1720.
Name of gatekeeper	Enter the IP address of the gatekeeper.
Port to communicate with gatekeeper	Enter the port on the gatekeeper with which the signaling port, or talker, will communicate in order to register with the gatekeeper. The default is 1719.
Password for use of gatekeeper	Enter the password, if any, associated with the gatekeeper.

H.323_Registration

Use this Knowledge Script to register a NetIQ endpoint computer (also called the signaling port or the talker) with a gatekeeper over H.323. Registration verifies the availability of the gatekeeper and allows a gatekeeper to map dialed numbers to an IP addressing structure.

You do not need to run this script before running the H.323_Listen script.The Listen script automatically performs registration if a gatekeeper is present.

The registration test returns one measurement: total response time for registering with a gatekeeper.

Tip
To monitor gatekeeper availability, run this script on the agent computer to register and deregister the agent computer with the gatekeeper.

Resource Object

H323Agent

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Collect data?	Select **y** to collect data for reports and graphs. The default is y.
Event severity when registration fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which registration fails. The default is 5.
Name or IP address of gatekeeper	Enter the name or IP address of the gatekeeper.
Port to communicate with gatekeeper	Enter the port on the gatekeeper with which the signaling port, or talker, will communicate in order to register with the gatekeeper. The default is 1719.
Password for use of gatekeeper	Enter the password, if any, associated with the gatekeeper.

H.323_UpdateAlias

Use this Knowledge Script to update the alias name of the H.323 resource in the repository. The alias name is the arbitrary name that you assigned the H.323 resource (the computer with the endpoint installed) when you configured it. By assigning an alias to the endpoint computer and then running H.323_UpdateAlias, you can pull all of the configured information into AppManager.

The new alias name is used when you stop and restart existing jobs or when you create new jobs. If you rerun the Discovery_VoIPQuality_CallSetup_H.323 Knowledge Script, the alias name is reset to the default name.

AppManager uses `<devicename>.netiq` as the default alias for H.323 devices. If a router gateway requires an access list, consider changing the alias to an IP address or to a fully qualified hostname so that the router can locate the AppManager managed object.

Resource Object

H.323 object

Run this script on only one resource at a time.

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
New alias name	Enter a new alias name for the H.323 resource.
Event severity when update fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the update fails. The default is 5.

Report_H.323Configuration

Use this Knowledge Script to summarize Call Setup H.323 configuration information for the selected computers.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Data Source	
Select computer(s)	Select the computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Report Settings	
Include parameter card?	Select **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is H323Config.
Add job ID to output folder name?	Select **y** to append the job ID to the name of the output folder. The default is n. A job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Select report properties in the Report Properties dialog box. The default report name is Call Setup H.323 Configuration Report.
Add time stamp to title?	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Select **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_H.323ResponseAvailMatrix

Use this Knowledge Script to summarize the average H.323 response time and availability between a talker and a listener within a time frame that you select.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Data Source	
Select Knowledge Script(s)	Select the Knowledge Scripts to include in the report.
Select computer(s)	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding
Report Settings	
Decimal accuracy for % values	Specify the number of decimal places that you want to see in the values generated by this report. The default is 3.
Include parameter card?	Select **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is H323RespAvailMatrix.
Add job ID to output folder name?	Select **y** to append the job ID to the name of the output folder. The default is n. A job ID lets you correlate a specific instance of a Report script with the corresponding report.
Select properties	Set the report properties as desired. The default report name is Call Setup H.323 Response Time Availability.
Add time stamp to title?	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Select **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.

Parameter	How To Set It
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_H.323ResponseTimeDetail

Use this Knowledge Script to summarize the average H.323 response time by minute within a time range that you select.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Data Source	
Select Knowledge Script(s)	Select the Knowledge Scripts to include in the report.
Select computer(s)	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Aggregate by n minute(s)	Enter the number of minutes in which time period data will be grouped. The default is 15 minutes.
Report Settings	
Include parameter card?	Select **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Select **y** to include a chart in the report. The default is y.
Include table?	Select **y** to include a table of information in the report. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is H323RespTimeDetail.
Add job ID to output folder name?	Select **y** to append the job ID to the name of the output folder. The default is n. A job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Set the report properties as desired. The default report name is Call Setup H.323 Response Time Detail.
Add time stamp to title?	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	

Parameter	How To Set It
Raise event if report succeeds?	Select **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_SIPConfiguration

Use this Knowledge Script to summarize SIP call setup configuration information for the selected computers.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Data Source	
Select computer(s)	Select the computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Report Settings	
Include parameter card?	Select **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is SIPConfig.
Add job ID to output folder name?	Select **y** to append the job ID to the name of the output folder. The default is n. A job ID lets you correlate a specific instance of a Report script with the corresponding report.
Select properties	Set the properties parameters as desired. The default report name is Call Setup SIP Configuration Report.
Add time stamp to title?	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Select **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_SIPResponseAvailMatrix

Use this Knowledge Script to summarize the average SIP response time and availability between a talker and a listener within a time frame that you select.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Data Source	
Select Knowledge Script(s)	Select the Knowledge Scripts to include in the report.
Select computer(s)	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding
Report Settings	
Decimal accuracy for % values	Enter the number of decimal places that you want to see in the values generated by this report. The default is 3.
Include parameter card?	Select **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is SIPRespAvailMatrix.
Add job ID to output folder name?	Select **y** to append the job ID to the name of the output folder. The default is n. A job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Set the report properties as desired. The default report name is Call Setup SIP Response Time Availability.
Add time stamp to title?	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Select **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.

Parameter	How To Set It
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_SIPResponseTimeDetail

Use this Knowledge Script to summarize the average SIP response time by minute within a time range that you select.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Data Source	
Select Knowledge Script(s)	Select the Knowledge Scripts to include in the report.
Select computer(s)	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Aggregate by n minute(s)	Enter the interval in minutes in which time period data will be grouped. The default is 15 minutes.
Report Settings	
Include parameter card?	Select **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Select **y** to include a chart in the report. The default is y.
Include table?	Select **y** to include a table of information in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Line.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is SIPRespTimeDetail.
Add job ID to output folder name?	Select **y** to append the job ID to the name of the output folder. The default is n. A job ID lets you correlate a specific instance of a Report script with the corresponding report.
Select properties	Set the report properties as desired. The default report name is Call Setup SIP Response Time Detail.
Add time stamp to title?	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.

Parameter	How To Set It
Event Notification	
Raise event if report succeeds?	Select **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

SIP_CallSetup_Direct

Use this Knowledge Script to perform all of the steps associated with setting up a VoIP call using SIP directly between two endpoints: 1) send a SIP `INVITE` message to the listener endpoint, 2) encapsulate media information, including codec and RTP ports in the body of the `INVITE` message using SDP, and 3) process the server's response to determine whether the call was successfully initiated.

This script raises an event when response time exceeds the threshold that you set.

You can set up SIP call across a LAN to ensure that a SIP device can make direct calls. This "loop back" monitoring job list you verify proper installation and configuration of SIP agent devices. In addition, you can determine the response time, which indicates LAN performance, for SIP call setup between client devices.

Prerequisites

- Run SIP_Listen to verify that the endpoint is available and capable of receiving incoming calls.
- This script assumes that the SIP registrar has the same IP address as the proxy agent computer.

Resource Object

SIP object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Collect data?	Select **y** to collect data for reports and graphs. The default is y.
Select listener(s)	Select the names of the computers that you want to act as listeners.
Threshold - Maximum response time	Specify the maximum amount of response time that can occur before an event is raised. The default is 800 milliseconds.
Event severity when response time exceeds the threshold	Set the severity level, from 1 to 41, to indicate the importance of an event in which response time exceeds the threshold. The default is 15.
Event severity when SIP call is unsuccessful	Set the severity level, from 1 to 41, to indicate the importance of an event in which the SIP call does not complete successfully. The default is 5.
Talker port number	Enter the port number of the talker computer. The default is 5060.
Listener port number	Enter the port number of the listener computer. The default is 5060.

SIP_CallSetup_Server

Use this Knowledge Script to perform all of the steps associated with setting up a VoIP call that is routed from one endoint to another through a SIP server.

- First, the script sends a SIP `INVITE` message to the listener endpoint via a SIP server.
- *If the SIP server is a proxy server*, then the script performs all signaling functions through the proxy.
- *If the SIP server is a redirect server*, then the script parses the new URL (in the Contact field) and contacts that server to actually set up the call.
- Next, the script encapsulates media information, including codec and RTP ports in the body of the `INVITE` message using SDP.
- Finally, the script processes the server's response to determine whether the call was successfully initiated.

This script raises an event when response time exceeds the threshold that you set.

Prerequisites

- Run SIP_Listen, which verifies that the endpoint is available and capable of receiving incoming calls.
- This script assumes that the SIP registrar has the same IP address as the proxy agent computer.

Resource Object

SIPAgent

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Collect data?	Select **y** to collect data about response time for reports and graphs. The default is y.
Select listener(s)	Select the names of the computers that you want to act as listeners.
Threshold - Maximum response time	Specify the maximum amount of response time that can occur before an event is raised. The default is 800 milliseconds.
Event severity when response time exceeds the threshold	Set the severity level, from 1 to 41, to indicate the importance of an event in which response time exceeds the threshold. The default is 15.
Event severity when SIP call is unsuccessful	Set the severity level, from 1 to 41, to indicate the importance of an event in which the SIP call does not complete successfully. The default is 5.
Talker port number	Enter the port number of the talker computer. The default is 5060.
Listener port number	Enter the port number of the listener computer. The default is 5060.
Name or IP address of proxy	Enter the name or IP address of the proxy computer.

Parameter	How To Set It
Proxy port number	Enter the port number of the proxy computer. The default is 5060.
Register talker with proxy?	Enter **y** to register the talker computer with the proxy computer. The default is n.

SIP_Listen

Use this Knowledge Script to start a new thread, open a specified port, listen for incoming SIP messages, and then automatically return a response that indicates success. If necessary, the test registers the SIP endpoint with a SIP server so that the SIP endpoint can receive incoming calls in a server-based environment. SIP_Listen continues to run asynchronously until the job is stopped. It polls the endpoint every 60 seconds and refreshes the registration, if necessary, and it issues a `stop listen` command when the job is stopped.

Prerequisite

This script assumes that the SIP registrar has the same IP address as the proxy agent computer.

Resource Object

SIPAgent

Default Schedule

By default, this script runs on an asynchronous schedule. Regardless of the schedule that you select, once you start the script, its job status appears as Running.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Event severity when registration fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which registration is unsuccessful. The default is 5.
Listener port number	Enter the port number of the listener computer. The default is 5060.
Name or IP address of proxy	Enter the name or IP address of the proxy computer.
Proxy port number	Enter the port number of the proxy computer. The default is 5060.

SIP_Registration

Use this Knowledge Script to perform basic registration with the server and checks for response time, a valid response, and a successful return code. Upon completion, this script immediately deregisters with the server by sending a `REGISTER` request with a TTL of **0**.

You do not need to run this script before running SIP_Listen. The Listen script automatically performs registration.

This script raises an event when response time exceeds the threshold that you set.

Prerequisite

This script assumes that the SIP registrar has the same IP address as the proxy agent computer.

Resource Object

SIP object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Collect data?	Select **y** to collect data about response time for reports and graphs. The default is y.
Threshold - Maximum response time	Specify the maximum amount of response time that can occur before an event is raised. The default is 800 milliseconds.
Event severity when response time exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which response time exceeds the threshold. The default is 15.
Event severity when registration fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which registration fails. The default is 5.
Registrant port number	Enter the port number of the computer that you want to register. The default is 5060.
Name or IP address of proxy	Enter the name or IP address of the proxy computer.
Proxy port number	Enter the port number of the proxy computer. The default is 5060.

SIP_UpdateAlias

Use this Knowledge Script to update the alias or DNS name of the SIP resource in the repository. You can drop this script on only one resource at a time. Once you update the alias/DNS name, the new name is used when you stop and restart existing jobs or when you create new jobs. If you rerun the Discovery_VoIPQuality_CallSetup_SIP script, the alias/DNS name is reset to the default name.

Note
The alias/DNS name is the arbitrary name you assigned the SIP resource (the computer with the endpoint installed) when you configured it. To pull all configured information into AppManager, assign an alias/DNS name to the endpoint computer and then run SIP_UpdateAlias.

Prerequisite

This script assumes that the SIP registrar has the same IP address as the proxy agent computer.

Resource Object

SIP object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
New alias name	Provide a new alias name for the SIP resource. You can enter an alias name in addition to a DNS name or instead of a DNS name.
New DNS name	Provide a new DNS name for the SIP resource. You can enter a DNS name in addition to an alias name or instead of an alias name.
Event severity when update fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the alias update fails. The default is 5.

Chapter 18
CiscoCallMgr Knowledge Scripts

AppManager Knowledge Scripts help you monitor and regulate services that are critical to Cisco CallManager performance. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AnalogOutboundBusy	Monitors the number of times during an interval that a call was attempted through an analog access when no ports were available.
AnalogPortsActive	Monitors active ports.
AnalogPortsOutOfService	Monitors out-of-service ports.
CallActivity	Monitors call activity on selected CallManagers.
CallFailures	Monitors Call Detail Records for calls that have an abnormal cause of termination.
CallQuality	Monitors the calls recorded in the Call Management Records for jitter, latency, lost data, and listening MOS.
CallsActive	Monitors active calls.
CallsAttemptedByPhone	Monitors calls attempted by an individual phone.
CallsInProgress	Monitors the number of calls in progress and the percentage of in-progress calls that are active.
CCM_CheckFirmware	Detects any device that is not using the default firmware load. Replaces the need to launch the Cisco CallManager Administration Web page in order to determine the same information.
CCM_CpuHigh	Monitors CPU usage for CallManager processes.
CCM_DeviceStatus	Monitors the status of up to 100 key phones within a cluster.
CCM_EventLog	Monitors event log entries from CallManager during the past *n* hours.
CCM_FXOPorts	Monitors active and in-service FXO ports for a CallManager.
CCM_FXSPorts	Monitors active and in-service FXS ports for a CallManager.
CCM_HealthCheck	Monitors the status of CallManager services.
CCM_HeartBeat	Monitors the CallManager heartbeat. A low heartbeat indicates the CallManager service was stopped and then restarted.
CCM_MemByProcess	Monitors individual memory use for each specified process, and the total memory use for all specified processes.
CCM_MemoryHigh	Monitors memory usage and memory pool usage of specified CallManager processes.

Knowledge Script	What It Does
CCM_MOHUnavailable	Monitors the number of times an attempt was made to allocate a Music On Hold resource when all MOH servers were active or when no MOH servers were registered.
CCM_PhoneCheck	Monitors your CallManager network for new and missing phones.
CCM_PhoneInventory	Takes an inventory of phones based on specified search criteria. You can choose to write the results to a file.
CCM_PRIChannels	Monitors active and in-service PRI channels for a CallManager.
CCM_Replication	Queries for failed actions in the history tables of the replication agents on the CallManager Publisher.
CCM_ResetDevice	Resets one or more devices in order for the devices to pick up new default firmware.
CCM_RestartService	Schedules a CallManager service to stop and then restart after a specified interval.
CCM_RoleStatus	Determines whether a CallManager's status is Primary or Backup. A Backup is defined as any CallManager with no registered phones (hardware or software).
CCM_SecureWebPageCheck	Monitors the ccmadmin and ccmuser Web pages for Cisco CallManager 4.1 and later.
CCM_SystemPerformance	Monitors call throttling, signals in queue, and severe and warning call-throttling states for a CallManager.
CCM_SystemUsage	Monitors average CPU and memory usage for all monitored CallManagers.
CCM_T1Channels	Monitors active and in-service T1-CAS channels for a CallManager.
CCM_WebPageCheck	Monitors up/down status and round-trip time for the ccmadmin and ccmuser Web pages. If you are monitoring CallManager 4.1 or later, use CCM_SecureWebPageCheck.
CDRQuery	Queries the CDR table on the CallManager Publisher.
CiscoBackupStatus	Monitors the status of the Cisco Backup Utility program (stiBack.exe) and the Cisco BARS program.
ConfBridgeActiveConf	Monitors active conferences for a Conference Bridge.
ConfBridgeActiveStreams	Monitors active streams for a Conference Bridge.
ConfBridgeAvailStreams	Monitors available streams for a Conference Bridge.
ConfBridgeConferences	Monitors completed conferences for a Conference Bridge.
ConfBridgeStreams	Monitors streams on completed conferences for a Conference Bridge.
CTI_Manager	Monitors CTI Manager connections, open devices, open lines, and active CallManager links.
DigitalOutboundBusy	Monitors the number of times during an interval that a call through a Digital Access was attempted when no ports were available.
DigitalPortsActive	Monitors active digital ports.
DigitalPortsOutOfService	Monitors out-of-service digital ports.
H323CallActivity	Monitors call activity on an H.323 device.
H323CallsAttempted	Monitors attempted calls for an H.323 device.
H323CallsInProgress	Monitors in-progress calls for an H.323 device.
IIS_CpuHigh	Monitors CPU usage for IIS application processes.

Knowledge Script	What It Does
IIS_HealthCheck	Monitors the queue length for blocked I/O requests and the up-and-down status of IIS services and Web sites.
IIS_KillTopCPUProcs	Monitors CPU usage of the dllhost and MTX processes.
IIS_MemoryHigh	Monitors memory usage and memory pool usage of specified IIS applications.
IIS_RestartServer	Restarts an IIS server.
IIS_ServiceUpTime	Monitors discovered Web sites and Web services uptime.
LineStatus	Monitors active calls for an individual line.
LocationBandwidth	Monitors the bandwidth statistics for a Location resource that has been defined in CallManager.
LocationOutOfBandwidth	Monitors the number of times calls through a Location failed due to lack of bandwidth.
LossOfHardwarePhones	Monitors registered hardware phones.
MGCP_FXO	Monitors call activity for MGCP FXO devices.
MGCP_FXS	Monitors call activity for MGCP FXS devices.
MGCP_Gateway_CCM30	Monitors station ports and voice channels for CallManager 3.0 MGCP gateway devices.
MGCP_Gateway_CCM31	Monitors station ports and voice channels for CallManager 3.1 (and higher) MGCP gateway devices.
MGCP_GatewayCheck	Monitors for new or missing MGCP gateways.
MGCP_PRI	Monitors call activity and data link availability for MGCP PRI devices.
MGCP_PRI_Channels	Monitors active and out-of-service channels for MGCP PRI devices.
MGCP_T1CAS	Monitors call activity and data link availability for MGCP T1-CAS devices.
MGCP_T1CAS_Channels	Monitors active and out-of-service channels for MGCP T1-CAS devices .
MLA_Logins	Scans the CallManager MLA log file for successful and failed logins during a specified interval.
MOHDevice	Monitors active and available resources for Music On Hold devices.
MOHServer	Monitors active and available streams for Music On Hold servers.
MOHServer_LostConnections	Monitors lost connections for Music On Hold servers.
MTP_Device	Monitors active and available resources for a Media Termination Point device.
MTPActiveConnections	Monitors active connections for a Media Termination Point.
MTPActiveStreams	Monitors active streams for a Media Termination Point.
MTPAvailableStreams	Monitors available streams for a Media Termination Point.
MTPCompletedConnections	Monitors completed connections for a Media Termination Point.
MTPCompletedStreams	Monitors streams on completed connections for a Media Termination Point.
MTPsActive	Monitors active Media Termination Points.
MTPsAvailable	Monitors available Media Termination Points.

Knowledge Script	What It Does
MTPsUnavailable	Monitors the number of times during an interval a Media Termination Point allocation was requested when none was available.
MulticastConfActive	Monitors active Multicast conferences.
MulticastConfAvailable	Monitors the number of new Multicast conferences that can be started.
MulticastConfCompleted	Monitors completed Multicast conferences.
MulticastConfPhones	Monitors active Multicast participants.
MulticastConfUnavailable	Monitors the number of times during an interval a Multicast conference was requested when none was available.
QRTEvent	Monitors the log files of the Quality Reporting Tool and starts a diagnostic action if a QRT request has been logged.
RegAnalogAccesses	Monitors registered analog accesses.
RegCtiPorts	Monitors CTI ports registered to the local CallManager.
RegDigitalAccesses	Monitors registered digital accesses.
RegHardwarePhones	Monitors registered hardware phones.
RegMGCPGateways	Monitors registered MGCP gateways.
RegOtherDevices	Monitors registered station devices using the SCCP protocol that are not hardware phones.
Report_CallActivity	Summarizes data relating to attempted and completed calls.
Report_CallQualityDailyAvg	Summarizes key call quality data: jitter, latency, and lost data.
Report_CallsByHour	Displays the number of active calls for all selected CallManagers.
Report_ClusterAvgValueByHr	Displays the average values by hour of the data stream(s) for all selected CallManager clusters.
Report_ClusterAvgValueByMin	Displays the average values by minute of the data stream(s) for the selected CallManager cluster.
Report_ClusterGenCounter	For a selected CallManager cluster, displays the average, maximum, and minimum values of each data stream, and the actual data values of each data stream over time.
Report_ClusterSystemUsage	For a selected CallManager cluster, displays the average CPU and memory usage per CallManager.
Report_MGCPChannelUsage	Displays the number of total active and out-of-service voice channels for a particular MGCP PRI Group.
Report_MGCPDeviceUtil	Displays outbound busy attempts and completed calls for a particular MGCP device.
Report_MGCPGatewayUsage	Displays the number of active MGCP PRI Voice Channels for a particular gateway.
Report_ServicesAvailability	Summarizes the availability of the services most relevant to the selected CallManagers.
Report_SystemUsage	Displays the average CPU and memory usage for the selected CallManagers.
SQL_Accessibility	Monitors SQL Server and database accessibility.
SQL_BlockedProcesses	Monitors SQL processes that have been blocked for more than the specified period of time.
SQL_CPUUtil	Monitors CPU resources used by sqlservr and sqlagent processes.

Knowledge Script	What It Does
SQL_DataGrowthRate	Monitors data growth and shrink rates for all SQL Server databases.
SQL_DataSpace	Monitors available data space and used data space in a SQL Server 7.0 database.
SQL_DBGrowthRate	Monitors database growth and shrink rates.
SQL_DbOption	Checks the database option.
SQL_DBSpace	Monitors available database space and used database space in a SQL Server 7.0 database.
SQL_Errorlog	Monitors the SQL Server error log.
SQL_LogGrowthRate	Monitors log growth and shrink rates for all SQL Server databases.
SQL_LogSpace	Monitors available log space and log data space in a SQL Server 7.0 database.
SQL_MemUtil	Monitors the percentage of memory used by `sqlservr` and `sqlagent` processes.
SQL_NearFileMaxSize	Monitors the size of all SQL Server database files.
SQL_NearMaxConnect	Monitors the percentage of used user connections.
SQL_NearMaxLocks	Monitors the lock usage of SQL Server.
SQL_NetError	Monitors SQL Server network packet errors.
SQL_RepTransactions	Monitors transactions in the transaction log of the publication database that are marked for replication but have not been replicated.
SQL_RepTranSec	Monitors transactions being replicated per second.
SQL_RestartServer	Restarts a down SQL Server.
SQL_ServerDown	Monitors the up-and-down status of SQL Server.
SQL_ServerThroughput	Monitors the throughput of SQL Server by measuring the number of T-SQL batch requests executed per second and the number of physical page reads per second.
SQL_TopIOUsers	Monitors I/O read-and-write operations used by SQL Server users and their connections.
SQL_TopLockUsers	Monitors locks held by all SQL Server users and their connections.
SQL_TopMemoryUsers	Monitors the memory that can be allocated to all SQL Server users and their connections in 2-KB pages.
SQL_UserConnections	Monitors SQL Server user connections.
StreamAppIOCTLErr	Monitors the number of times in an interval an IOCTL error was detected.
StreamAppMissDDErr	Monitors the number of times in an interval a missing device driver error was detected.
TftpChangeNotify	Monitors handled TFTP change notifications.
TftpErrors	Monitors TFTP-related errors.
TftpHeartBeat	Monitors the Cisco TFTP heartbeat.
TftpRequests	Monitors handled TFTP requests.
TftpSegmentPctLost	Monitors lost TFTP segments.
TftpSegmentsSent	Monitors sent TFTP segments.

Knowledge Script	What It Does
TraceArchive	Archives CallManager trace files to prevent losing files when tracing wraps.
TraceEvent	Scans CallManager trace files for entries that match a text string you specify.
Transcoder_Device	Monitors active and available resources for an individual transcoder device.
TranscoderResources	Monitors transcoder resources between the G.711, G.723, and G.729 codecs.
TranscoderUnavailable	Monitors the number of times during a specified period a transcoder resource was requested when none was available.
UnicastConfActive	Monitors active Unicast conferences.
UnicastConfAvailable	Monitors the number of new Unicast conferences that can be started.
UnicastConfBridge_Device	Monitors active and available resources for an individual software or hardware conference bridge device.
UnicastConfComplete	Monitors completed Unicast conferences.
UnicastConfParticipants	Monitors active Unicast participants.
UnicastConfUnavailable	Monitors the number of times in an interval a Unicast conference was requested when none was available.
VerifyPasswords	Verifies the sa, Administrator, and Directory Manager passwords on a CallManager computer.
Recommended Knowledge Script Groups	Run all recommended Knowledge Scripts at one time.

AnalogOutboundBusy

Use this Knowledge Script to monitor the number of times a call was attempted through an analog access when no ports were available. This script raises an event if the number of outbound busy attempts exceeds the threshold. In addition, this script generates a data stream for outbound busy attempts.

Resource Object

CCM Analog Access object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of outbound busy attempts exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about outbound busy attempts for reports and graphs. The default is n.
Threshold - Maximum outbound busy attempts	Specify the maximum number of outbound busy attempts can occur before an event is raised. The default is 100 calls.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of outbound busy attempts exceeds the threshold. The default is 25.

AnalogPortsActive

Use this Knowledge Script to monitor the number of active ports. This script raises an event if the number of active ports exceeds the threshold. In addition, this script generates a data stream for the number of active ports.

Resource Object

CCM Analog Access object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of active ports exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about active ports for reports and graphs. The default is n.
Threshold - Maximum active ports	Specify the maximum number of ports that can be active before an event is raised. The default is 20 ports.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active ports exceeds the threshold. The default is 25.

AnalogPortsOutOfService

Use this Knowledge Script to monitor the number of ports that are out of service. This script raises an event if the number of out-of-service ports exceeds the threshold. In addition, this script generates a data stream for out-of-service ports.

Resource Object

CCM Analog Access object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of out-of-service ports exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about out-of-service ports for reports and graphs. The default is n.
Threshold - Maximum out-of-service ports	Specify the maximum number of ports that can be out of service before an event is raised. The default is 2 ports.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of out-of-service ports exceeds the threshold. The default is 15.

CallActivity

Use this Knowledge Script to monitor call activity (attempted, completed, and incomplete) during a specified time range.

This script collects the data used by the Report_CallActivity Knowledge Script.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs once each day.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to **y** to collect data about call activity for reports and graphs. The default is y.
Monitor completed calls?	Set to **y** to monitor completed calls. The default is y.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 500 calls.
Event severity when completed calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which completed calls exceed the threshold. Enter **0** if you do not want to raise an event. The default is 25.
Monitor attempted calls?	Set to **y** to monitor attempted calls, such as calls that received a busy signal or in instances when users leave the handset off the phone. The default is y.
Threshold - Maximum attempted calls	Specify the maximum number of calls that can be attempted before an event is raised. The default is 500 calls.
Event severity when attempted calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which attempted calls exceed the threshold. Enter **0** if you do not want to raise an event. The default is 25.
Monitor incomplete calls?	Set to **y** to monitor incomplete calls, such as calls that were attempted but did not complete or are not currently in progress. The default is y.
Threshold - Maximum incomplete calls	Specify the maximum percentage of incomplete calls can occur before an event is raised. The default is 75%.
Event severity when incomplete calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of incomplete calls exceeds the threshold. Enter **0** if you do not want to raise an event. The default is 25.

CallFailures

Use this Knowledge Script to monitor the Call Detail Records (CDR) in the CallManager Publisher database for calls that ended with an abnormal cause code.

If a Subscriber loses its connection to a Publisher, it will store its CDR data locally until the connection is restored. If the connection is not restored within the collection interval, this script may not monitor some calls.

Note
CallManager does not collect CDR records by default. You must enable the collection of CDRs for each CallManager is a cluster. From the Cisco CallManager Administration Web page, navigate to **Service > Service Parameters > CallManager**. Set the **CdrEnabled** parameter to **T**.

Resource Object

CCM Publisher

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if failed calls exceed the threshold?	Set to **y** to raise an event if the number of failed calls exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n. This parameter collects the total number of failed calls found during the time period you specify in the *Start time*, *Start date*, *Stop time*, and *Stop date* parameters. **Note** Some third-party billing applications remove CDR records from the CallManager database. If records are removed before the CallFailures script has a chance to run, the script will not collect any data.
CallManager database username	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Use Windows authentication?	Set to **y** to use Windows authentication to access the Publisher database. If you enable this parameter, the SQL user name is ignored. The `NetIQmc` service must be running with the proper authentication to access the database. The default is Yes.

Parameter	How to Set It
Threshold - Maximum failed calls	Specify the maximum number of calls that can fail before an event is raised. The default is 0 calls. **Note** You can trigger NetIQ Vivinet Diagnostics to diagnose the problem indicated by an event in which this threshold is exceeded. For more information, see “Diagnosing VoIP Quality” on page 813.
Include call details?	Set to **y** to include call details in the event message. The default is y. If set to y, the event message includes details for up to 50 calls. The call details can include any or all of the following: • Originator termination cause • Destination termination cause • Originating Party Device Name (if running on CallManager 3.1 or later) • Originating Party Directory Number • Originating Party Partition • Originating Party CallManager Node ID • Originating Party IP address • Originating Party codec • Destination Party Device Name (if running on CallManager 3.1 or later) • Destination Party Directory Number • Destination Party Partition • Destination Party CallManager Node ID • Destination Party IP address • Destination Party codec • Time the call was connected • Time the call was disconnected • Call duration
Directory number to filter by	Provide a directory number by which to filter the calls that get monitored. The default is to monitor all calls. You can specify a group of directory numbers by using the % wildcard. For example, to monitor all the directory numbers that begin with 31, enter 31%. **Note** This parameter returns results only if the directory number you enter is the originator's number. No results are returned if you enter the destination number.
Exclude these failure codes	Provide a comma-separated list of termination codes that are not to be considered failures. For more information, see “Termination Codes” on page 814. **Note** Codes 0, 16, 31, and 127 are automatically excluded. They are normal termination codes. However, these codes may appear in events if the other side of the call has a failure code that has not been excluded.
Minimum call duration	Specify the minimum number of seconds for which a call must be connected before the script checks whether the call has failed and includes it in the query. The default is 0 seconds.
Start date	Specify the date on which you want to start the query. This parameter is valid only when you select **Run Once** on the Schedule tab.
Start time	Specify the time at which you want to start the query. This parameter is valid only when you select **Run Once** on the Schedule tab.

Parameter	How to Set It
Stop date	Specify the date on which you want to stop the query. This parameter is valid only when you select **Run Once** on the Schedule tab.
Stop time	Specify the time at which you want to stop the query. This parameter is valid only when you select **Run Once** on the Schedule tab.
Query timeout	Specify the maximum number of seconds it can take a query to run. The default is 10 seconds. **Note** The script runs three queries in order to get data for each interval.
Monitoring offset	Because CallManager can have a delay when writing records to the database, a query may not return any call failures if the script is monitoring only the past few seconds. Use this parameter to have the script offset the monitoring period in order to capture those failures that occurred earlier. The default is 45 seconds. For example, if the delay for writing CDR data to the database is 10 minutes, enter 600 in this field. The script will then query for calls that ended 10 minutes ago, rather than for calls that ended at the current time.
Event severity when failed calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 15.
Event severity when no records found	Set the severity level for an event in which the query finds no records. This is not the same event as finding no failed calls; this means there were no CDR records in the database for the given query. Accept the default of **0** if you do not want to raise an event. **Note** Set this parameter only to verify CDRs are actually being collected in a timely manner.

Diagnosing VoIP Quality

You can trigger NetIQ Vivinet Diagnostics to run a diagnosis of VoIP quality between two phones or two endpoints. A diagnosis is performed when one of the following Knowledge Scripts determines VoIP quality or call quality is poorer than a specified threshold:

- CallQuality. Vivinet Diagnostics can diagnose the problem when jitter, latency, and percentage of lost data exceed their thresholds.
- CallFailures. Vivinet Diagnostics can diagnose the problem when the number of failed calls exceeds its threshold.

The Action script runs by default only if Vivinet Diagnostics version 1.1 or later is installed on the computer on which the script is running.

For more information about Vivinet Diagnostics and VoIP quality diagnoses, see the *User Guide for Vivinet Diagnostics* and the Help for the Action_DiagnoseVoIPQuality Knowledge Script.

To trigger Vivinet Diagnostics:

1. On the Actions tab, click **Properties**.
2. Enter values for all parameters. For more information about the parameter values, click **Help** on the Properties for Action_DiagnoseVoIPQuality dialog box.
3. Continue entering values on the other tabs of the Properties dialog box, or click **OK** to run the job.

Termination Codes

Termination Code	Description	Explanation
0	No error	No error.
1	Unallocated (unassigned) number	Indicates the called party cannot be reached because, although the called party number is in a valid format, it is not currently allocated (assigned).
2	No route to specified transit network (national use)	Indicates one of the following: • The equipment sending this code has received a request to route the call through a particular transit network it does not recognize. The equipment does not recognize the transit network either because the transit network does not exist or because the transit network exists but does not serve the equipment that is sending the code. • The prefix 0 is invalid for the entered number.
3	No route to destination	Indicates one of the following: • The called party cannot be reached because the network through which the call has been routed does not service the desired destination. This cause is supported on a network-dependent basis. • A 1 was dialed when not required. Redial without the 1.
4	Send special information tone	Indicates one of the following: • The prefix 1 is not required for this number. • The called party cannot be reached for reasons are of a long-term nature. The special information tone should be returned to the calling party.
5	Misdialed trunk prefix (national use)	Indicates the erroneous inclusion of a trunk prefix in the called party number.
6	Channel unacceptable	Indicates a called user cannot negotiate for a B-channel other than that specified in the SETUP message.
7	Call awarded and being delivered in an established channel	Indicates the user has been awarded the incoming call and Indicates the call is being connected to a channel (such as packet mode or X.25 virtual calls) already established to that user for similar calls.
8	Pre-emption	Indicates a call has been preempted.
9	Preemption - circuit reserved for reuse	Indicates a call has been preempted because the circuit is reserved for reuse.
16	Normal call clearing	Indicates normal call clearing has occurred.
17	User busy	Indicates the called party is unable to accept another call because the user busy condition has been encountered. Code 17 may be generated by the called user or by the network. In the case of user-determined user busy, it is noted the user equipment is compatible with the call.
18	No user responding	Indicates a called party does not respond to a call establishment message with either an alerting or connect indication within the allotted prescribed period of time (before timer T303 or T310 has expired).
19	No answer from user (user alerted)	Indicates the called user has provided an alerting indication, but not a connect indication within a prescribed period of time (before timer T301 has expired).

Termination Code	Description	Explanation
20	Subscriber absent	Indicates one of the following:· • A mobile station has logged off. • Radio contact is not obtained with a mobile station. • A personal telecommunications user is temporarily not addressable at any user-network interface.
21	Call rejected	Indicates one of the following: • The equipment sending this cause does not wish to accept the call, although it could have accepted the call because it is neither busy nor incompatible. • May be generated by the network, indicated the call was cleared due to a supplementary service constraint.
22	Number changed	Indicates the called party number indicated by the calling party is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this cause, cause #1 shall be used.
26	Non-selected user clearing	Indicates the user has not been awarded the incoming call.
27	Destination out of order	Indicates the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" Indicates a signal message was unable to be delivered to the remote party, as in the following examples: • Physical layer or data link layer failure at the remote party • User equipment off-line
28	Invalid number format (address incomplete)	Indicates one of the following: • The called party cannot be reached because the called party number is not in a valid format or is not complete. • The user should be returned a Special Intercept Announcement.
29	Facility rejected	Indicates one of the following: • The network cannot provide the requested facility. • A user in a special business group, such as a Centrex, dialed an undefined code.
30	Response to STATUS ENQUIRY	Indicates one of the following: • This cause is included in the Status Message when the reason for sending the Status Message was the previous receipt of a Status Enquiry message. • A user from outside a basic business group, such as a Centrex, has violated an access restriction feature.
31	Normal, unspecified	Used to report a normal event only when no other cause in the normal class applies.
34	No circuit/channel available	Indicates no appropriate circuit or channel is available to handle the call.
38	Network out of order	Indicates the network is not functioning correctly and the condition is likely to last a relatively long time. Immediately re-attempting the call is not likely to be successful.
39	Permanent frame mode connection out of service	Indicates a permanent connection was terminated, probably due to equipment failure.

Termination Code	Description	Explanation
40	Permanent frame mode connection operational	Indicates a permanent connection is operational again. The connection was previously terminated, probably due to equipment failure.
41	Temporary failure	Indicates the network is not functioning correctly and the condition is not likely to last a long time. The user may wish to attempt another call almost immediately. May also indicate a data link layer malfunction locally or at the remote network interface, or a call was cleared due to protocol error(s) at the remote network interface.
42	Switching equipment congestion	Indicates the switching equipment generating this cause is experiencing a period of high traffic.
43	Access information discarded	Indicates the network is unable to deliver user information (such as user-to-user information, low-level compatibility, or sub-address) to the remote users as requested.
44	Requested circuit/ channel not available	Indicates the other side of the interface cannot provide the circuit or channel indicated by the requesting entity.
46	Precedence call blocked	Indicates the remote device that was called is busy.
47	Resource unavailable, unspecified	Indicates one of the following: • No other cause in the resource unavailable class applies. • The original destination is unavailable. Invoke redirection to a new destination.
49	Quality of Service not available	Indicates the network cannot provide the requested Quality of Service. May be a subscription problem.
50	Requested facility not subscribed	Indicates this facility is unavailable because the user has not subscribed to it.
53	Service operation violated	Indicates the user has violated the service operation.
54	Incoming calls barred	Indicates the user will not accept the call delivered in the SETUP message.
55	Incoming calls barred within CUG (Closed User Group)	Indicates the network does not allow the user to receiver calls.
57	Bearer capability not authorized	Indicates the user has requested a bearer capability that is implemented by the equipment that generated this cause, however the user is not authorized to use it. This common problem is caused by incorrect Telco provisioning of the line at the time of installation.
58	Bearer capability not presently available	Indicates the user has requested a bearer capability that is implemented by the equipment that generated this cause, however the bearer capability is unavailable at the present time. This problem may be due to a temporary network problem or a subscription problem.
62	Inconsistency in designated outgoing access information and subscriber class	Indicates an inconsistency in the designated outgoing access information and subscriber class.
63	Service or option not available, unspecified	Indicates a service or option is not available. Used only when no other cause in this class applies.
65	Bearer capability not implemented	Indicates the equipment sending this cause does not support the requested bearer capability.

Termination Code	Description	Explanation
66	Channel type not implemented	Indicates the called party has reached an unsupported channel type.
69	Requested facility not implemented	Indicates the network (or node) does not support the requested bearer capability and therefore cannot be accessed at this time.
70	Only restricted digital information bearer capability is available (national use)	Indicates the calling party has requested an unrestricted bearer service, however the equipment sending this cause only supports the restricted version of the requested bearer capability.
79	Service or option not implemented, unspecified	Indicates a service or option was not implemented. Used only when no other cause in this class applies.
81	Invalid call reference value	Indicates the equipment sending this cause has received a message with a call reference that is not currently in use on the user-network interface. This value applies only if the call reference values 1 or 2 octets long and is not the global call reference.
82	Identified channel does not exist	Indicates the equipment sending this cause has received a request to use a channel that is not active on the interface for a call.
83	A suspended call exists, but this call identity does not	Indicates a suspended call exists but the call's identity does not.
84	Call identity in use	Indicates a call identity is in use.
85	No call suspended.	Indicates no call is suspended.
86	Call having the requested call identity has been cleared	Indicates the call having the requested call identity has cleared.
87	User not member of CUG (Closed User Group)	Indicates the call was not completed, probably due to one of the following reasons: • The dialed number is incorrect • The user is not authorized to use (or has not subscribed to) the requested service • User is using a service that the remote device is not authorized to use
88	Incompatible destination	Indicates the equipment sending this cause has received a request to establish a call that has low layer compatibility, high layer compatibility, or other compatibility attributes (such as data rate or DN subaddress), which cannot be accommodated. This call can be returned by a switch to a CPE when trying to route a call to an incompatible facility, or one without a data rate.
90	Destination number missing and DC not subscribed Nonexistent CUG (Closed User Group)	Indicates the call was not completed, probably due to one of the following reasons: • The dialed number is incorrect • The user is not authorized to use (or has not subscribed to) the requested service • User is using a service that the remote device is not authorized to use
91	Invalid transit network selection (national use)	Indicates an invalid transit network selection has been requested.
95	Invalid message, unspecified	Indicates the entity sending this cause has received an invalid message. Used when no other cause in this class applies.

Termination Code	Description	Explanation
96	Mandatory information element is missing	Indicates the equipment sending this cause has received a message that is missing an information element that must be present in the message before the message can be processed.
97	Message type non-existent or not implemented	Indicates one of the following: • The equipment sending this cause has received with a message type it does not recognize. Either the message is not defined, or it is defined and not implemented by the equipment sending this cause. • A problem with the remote configuration or with the local D-channel.
98	Message is not compatible with the call state, or the message type is non-existent or not implemented	Indicates one of the following: • Message received is not compatible with the call state • Message type is non-existent or not implemented
99	An information element or parameter does not exist or is not implemented	Indicates the equipment sending this cause has received a message that includes information elements not recognized because either the information element identifier is not defined, or it is defined but not implemented by the equipment sending the cause. However, the information element is not required for the equipment sending the cause to process the message.
100	Invalid information element contents	Indicates the equipment sending this cause has received an information element it has implemented. However, one or more fields of the information elements are coded in such a way (such as truncated, invalid extension bit, invalid field values) that the information element has not been implemented by the equipment that is sending this cause.
101	The message is not compatible with the call state	Indicates one of the following: • The equipment sending this cause has received a message the procedures indicate is not a permissible message to receive at this time. • The switch sending this cause is clearing the call because a threshold has been exceeded for multiple protocol errors during an active call.
102	The call was terminated when a timer expired and a recovery routine was executed to recover from the error	Indicates a procedure has been initiated by the expiration of a timer in associated with error-handling procedures.
103	Parameter non-existent or not implemented - passed on (national use)	Indicates the equipment sending this cause has received a message that includes parameters not recognized because the parameters are defined but not implemented by the equipment sending the cause. The parameters were ignored. In addition, if the equipment sending this cause is an intermediate point, this cause Indicates the parameters were passed on unchanged.
110	Message with unrecognized parameter discarded	Indicates the equipment sending this cause has discarded a received message that includes a parameter that is not recognized.

Termination Code	Description	Explanation
111	Protocol error, unspecified	Reports a protocol error event only when no other cause in this class applies.This cause may be displayed if the user failed to dial a 9 or an 8 for an outside line. In addition, this cause may be returned in the event of certain types of restrictions as to number of calls.
126	Call split	A Cisco-specific code. Indicates a call was terminated during a transfer operation because it was split off and terminated (not part of the final transferred call). This code can help determine which calls were terminated as part of a transfer operation.
127	Internetworking, unspecified	Indicates an internetworking call (usually a call to SW56 service) has ended. May also be seen in the event of a non-specific rejection by a long distance carrier.

CallQuality

Use this Knowledge Script to monitor Call Management Records (CMRs) for information about the amount of data that is sent and received, and for information about jitter, latency, lost data, and listening MOS.

This script raises an event if a monitored value exceeds or falls below the threshold you set. In addition, this script generates data streams for average jitter, latency, lost data (%), and average and minimum listening MOS.

Cisco CallManager defines lost data, jitter, latency, and listening MOS as follows:

- *Lost data* equals the total number of real-time transport protocol (RTP) data packets that have been lost since the beginning of reception. This number is defined as the number of packets that were expected minus the number of packets that were actually received. The number of packets received includes those that were late or duplicates. Packets that arrive late are not counted as lost; the presence of duplicate packets could result in a negative lost data amount. AppManager records any negative value as zero (0).
- *Jitter* is an estimate of the statistical variance of the RTP data packet interarrival time, measured in milliseconds and expressed as an unsigned integer. Interarrival jitter is the mean deviation (smoothed absolute value) of the difference in packet spacing at the receiver compared to the sender for a pair of packets.
- *Latency* is an estimate of network latency, expressed in milliseconds. Latency is the average value of the difference between the NTP time stamp indicated by the senders of the RTCP messages and the NTP timestamp of the receivers, measured when the messages are received. In a CMR, the average is obtained by adding all of the estimates, then dividing by the number of RTCP messages that have been received.
- *Listening MOS* (Mean Opinion Score) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. In a CMR, the MOS is based on measured items plus jitter buffer size. The jitter buffer size is constant based on the codec. The term "listening" indicates the MOS value does not include "conversational" characteristics such as delay.

Notes

- When a Subscriber loses its connection to the Publisher, it stores its CMR data locally until the connection is restored. If the connection is not restored within the collection interval, this script may not monitor some calls.
- When a Subscriber is flooded with calls, it throttles the number of calls that get returned to the Publisher at one time; some calls may not get monitored.
- The clocks on the Subscriber must be synchronized with those of the Publisher.
- CallManager writes CMRs only for Cisco IP phones and for gateways that use the MGCP (Media Gateway Control Protocol) to interface with CallManager.

Resource Object

CCM Publisher. Although you can run this script on the parent CallManager object, it will actually run only on the Publisher.

Default Schedule

By default, this script runs every five minutes.

Troubleshooting Hint

You can use this script as a troubleshooting tool for checking problems with an individual extension. Set the Schedule to "Run Once," set *Maximum acceptable jitter* to "0," set *Include call details* to "**Yes**," set *Call disconnect time range* to cover the time when the poor quality calls occurred, and set *Directory number to filter by* to the extension that has the problems. The details that are returned will include the IP address of the phone extension displayed as a link. If the phone supports it, click on this link to reveal some lower-level details about the phone.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CallQuality job fails. The default is 5.
CallManager database user name	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Use Windows authentication?	Select **Yes** to use Windows authentication to access the Publisher database. If you enable this parameter, the SQL user name is ignored. The `NetIQmc` service must be running with the proper authentication to access the database. The default is Yes.

Parameter	How to Set It
Include call details?	Select **Yes** to include details for up to 50 calls in the Message tab of the Event Properties dialog box. The default is Yes. The call details can include any or all of the following: • Originating Party Device Name (If running on CallManager 3.1)· • Originating Party Directory Number • Originating Party Partition • Originating Party CallManager Node ID • Time the call was completed • Jitter • Latency • Lost Data Percentage • Packets Sent • Packets Received • Packets Lost • Originating Party IP address • Originating Party codec • Destination Party Device Name (If running on CallManager 3.1) • Destination Party Directory Number • Destination Party Partition • Destination Party CallManager Node ID • Destination Party IP address • Destination Party codec • Call Duration
Monitor Jitter, Latency, and Percent Lost Data	
Event Notification	
Raise event if jitter, latency, or percent lost data exceeds threshold?	Select **Yes** to raise an event if the jitter, latency, or percent lost data values exceed the thresholds you set. The default is Yes.
Threshold - Maximum acceptable jitter	Specify the maximum amount of jitter that must occur before an event is raised. The default is 60 milliseconds. **Note** You can trigger Vivinet Diagnostics to diagnose the problem indicated by an event in which the jitter threshold is exceeded. For more information, see “Diagnosing VoIP Quality” on page 813.
Threshold - Maximum acceptable latency	Specify the maximum amount of latency that must occur before an event is raised. The default is 400 milliseconds. **Note** You can trigger Vivinet Diagnostics to diagnose the problem indicated by an event in which the latency threshold is exceeded. For more information, see “Diagnosing VoIP Quality” on page 813.
Threshold - Maximum acceptable percent lost data	Specify the maximum percentage of data that must be lost before an event is raised. The default is 1%. **Note** You can trigger Vivinet Diagnostics to diagnose the problem indicated by an event in which the percentage lost data threshold is exceeded. For more information, see “Diagnosing VoIP Quality” on page 813.

Parameter	How to Set It
Threshold - Minimum lost packets, if lost data threshold is exceeded	Set this threshold *only* if you set a threshold for *Maximum acceptable percent lost data*. Use this parameter on occasions when lost data does exceed the threshold you set, but you do not want to raise an event unless a specific number of packets has also been lost. The default is 0 packets. For example, you have set *Maximum acceptable percent lost data* to 10%, and you have set this parameter to 5 packets. If the amount of lost data is 15%, but the number of lost packets is only 2, no event is raised. An event is raised only if the percentage of lost data AND the number of lost packets exceed the thresholds you set.
Event severity if jitter, latency, or percent lost data exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which one or more of the jitter, latency, and lost data thresholds have been exceeded. The default is 15.
Data Collection	
Collect data for jitter, latency, and percent lost data?	Select **Yes** to collect data for reports and graphs. If enabled, data collection generates data streams for average jitter, latency, and percent lost data for the monitoring interval. **Note** Some third-party billing applications remove CDR records from the CallManager database. If records are removed before the CallQuality script has a chance to run, the script will not collect any data.
Monitor Listening MOS	
Monitor Average Listening MOS	
Event Notification	
Raise event if average listening MOS for any call falls below threshold?	Select **Yes** to raise an event if the average listening MOS for any call falls below the threshold you set. The default is Yes.
Threshold - Average listening MOS	Specify the minimum value for average listening MOS that must occur for *any* call to prevent an event from being raised. The default is 3.60. Average listening MOS is defined as the running average of MOS scores (recorded at 8-second intervals) observed since the beginning of the call.
Event severity if average listening MOS for any call falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average listening MOS for any call falls below the threshold. The default is 15.
Data Collection	
Collect data for average listening MOS?	Select **Yes** to collect data for reports and graphs. If enabled, data collection generates a data stream for average listening MOS for the monitoring interval.
Monitor Minimum Listening MOS	
Event Notification	
Raise event if minimum listening MOS for any call falls below threshold?	Select **Yes** to raise an event if the lowest listening MOS for any call falls below the threshold you set. The default is unselected.
Threshold - Minimum listening MOS	Specify the lowest listening MOS value that must occur for *any* call to prevent an event from being raised. The default is 3.60. Minimum listening MOS is defined as the worst of the MOS scores (recorded at 8-second intervals) observed since the beginning of the call.

Parameter	How to Set It
Event severity if minimum listening MOS for any call falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the lowest listening MOS for any call falls below the threshold. The default is 15.
Data Collection	
Collect data for lowest listening MOS?	Select **Yes** to collect data for reports and graphs. If enabled, data collection generates a data stream for lowest listening MOS for the monitoring interval.
Query Filters	
Directory number to filter by	Specify a directory number to filter the calls that get monitored. The default is to monitor all calls. You can specify a group of directory numbers by using a '%' as a wildcard. For example, to monitor all the directory numbers that begin with 31, enter 31%. **Note** This parameter returns results only if the directory number you enter is the originating number. No results are returned if you enter the destination number.
Minimum call duration filter	Use this parameter to filter out calls whose duration is less than the specified value. The default is 0 seconds.
No Records Found Notifications	
Event severity when no records found	Set the severity level, from 1 to 40, to indicate the importance of an event in which no jitter, latency, or percent lost data records are found. Accept the default of **0** if you do not want to raise an event for this incident.
Event severity when no MOS records found	Set the severity level, from 1 to 40, to indicate the importance of an event in which no MOS records are found. Accept the default of **0** if you do not want to raise an event for this incident.
Troubleshooting	
Select call disconnect time range	Select a **Specific** (fixed) or **Sliding** date/time range in which to search for call failures. The default is Specific.
Query timeout	Specify the maximum number of seconds it can take a query to run. The default is 10 seconds. **Note** This script runs three queries in order to get data for each interval.
Monitoring offset	Because CallManager can have a delay when writing records to the database, a query may not return any call failures if the script is monitoring only the past few seconds. You can choose to have the script offset the monitoring period in order to capture those failures that occurred earlier. The default is 45 seconds. For example, if the delay for writing CDR data to the database is 10 minutes, enter 600 in this field. The script will then query for calls that ended 10 minutes ago, rather than for calls that ended at the current time.

CallsActive

Use this Knowledge Script to monitor the number of active calls. This script raises an event if the number of active calls exceeds the threshold you set.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs once each day.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about active calls for reports and graphs. The default is n.
Threshold - Maximum active calls	Specify the maximum number of calls that can be active before an event is raised. The default is 500 calls.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

CallsAttemptedByPhone

Use this Knowledge Script to monitor the number of calls attempted by an individual phone during an interval. This script raises an event if the number of attempted calls exceeds the threshold you set.

Resource Object

CCM Phone folder

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about attempted calls for reports and graphs. The default is n.
Phones, separated by comma w/no space	Provide a comma-separated list of the names of the phones you want to monitor for attempted calls.
Threshold - Maximum attempted calls	Specify the maximum number of calls that can be attempted before an event is raised. The default is 100 calls.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

CallsInProgress

Use this Knowledge Script to monitor the number of calls in progress and the percentage of in-progress calls that are active. A call is considered "in-progress" as soon as the receiver is lifted. A call is considered "active" once a connection is made.

This script raises an event if the number of in-progress calls exceeds the threshold or if the percentage of active in-progress calls falls below the threshold.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs once each day.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a monitored value exceeds or falls below the threshold you set. The default is y.
Collect data for calls in progress?	Set to **y** to collect data about in-progress calls for reports and graphs. The default is n.
Threshold - Maximum calls in progress	Specify the maximum number of calls that can be in progress before an event is raised. The default is 100 calls.
Event severity when in-progress calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-progress calls exceeds the threshold. The default is 25.
Collect data for active calls?	Set to **y** to collect data about active in-progress calls for reports and graphs. The default is n.
Threshold - Minimum active calls	Specify the minimum percentage of calls that can be active before an event is raised. The default is 10%. **Note** By seeing how many in-progress calls are active, you can determine whether any in-progress calls are simply stuck off-hook.
Event severity when active calls fall below the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of active in-progress calls falls below the threshold. Accept the default of **0** if you do not want to raise an event.

CCM_CheckFirmware

Use this Knowledge Script to detect any device that has been configured with a non-default firmware load. This script returns the number of devices of each device type — the same information you would retrieve when accessing the Cisco CallManager Administration Web page.

This script does not determine which firmware load a device is running.

Only AppManager administrators should run this script.

Resource Object

CCM Publisher

Default Schedule

By default, this script runs once each day.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Threshold - Maximum devices with non-default firmware load	Specify the maximum number of devices, from all selected device types, that can be configured for a non-default firmware load before an event is raised. The default is 0 devices.
Raise event when threshold is not exceeded?	Set to **y** to raise an event when the threshold is *not* exceeded. The default is y.
Event severity when threshold is not exceeded	Set the event severity level to indicate the importance of an event in which the threshold is *not* exceeded. Enter **0** if you do not want to raise an event for this situation. The default is 25. For more information, see "Event Messages for CCM_CheckFirmware" on page 829.
Event severity when threshold is exceeded	Set the event severity level to indicate the importance of an event in which the threshold is exceeded. Enter **0** if you do not want to raise an event for this situation. The default is 15.

Parameter	How to Set It
Check … types?	Set to n if you do not want to check any of the following types of devices. The default is y. • Analog Access • Analog Access WS-X6624 • Cisco 12 S • Cisco 12 SP • Cisco 12 SP+ • Cisco 30 SP+ • Cisco 30 VIP • Cisco IP Phone 7905 • Cisco IP Phone 7910 • Cisco IP Phone 7935 • Cisco IP Phone 7940 • Cisco IP Phone 7960 • Cisco ATA 186 • Cisco Conference Bridge WS-X6608 • Digital Access WS-X6608 • Digital Access+ • Media Termination Point WS-X6608 • VGC Gateway • 14-Button Line Expansion Module

Event Messages for CCM_CheckFirmware

Following are two common error messages, accompanied by an explanation, a likely cause, and any operator action that may be needed.

Devices using non-default firmware load exceed the threshold.

Explanation: The number of devices that are configured with a non-default firmware load is greater than the specified threshold. See the detailed event message for details of the devices not configured with a default firmware load.

Likely cause: Normal message when the threshold has been crossed.

Operator action: Notify your Cisco CallManager administrator that there are devices that are not configured for the default firmware load.

Internal error encountered.

Explanation: Errors were encountered while checking one or more of the selected devices. See the detailed event message for details about the error.

Likely cause: In most cases this message Indicates a COM interface was not available, either because the COM object has not been installed or is not registered.

Operator action: Verify the `dblx.dll` is installed and registered on the CallManager computer.

CCM_CpuHigh

Use this Knowledge Script to monitor the CPU resources that application processes are consuming. If application CPU utilization exceeds the thresholds you set, an event is raised. The script monitors CPU usage for each process individually and the total CPU usage for all processes. If a process is not found, the script assumes the process is not running, and reports zero as the CPU result.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if any threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about CPU usage for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.
Monitor the Cisco CallManager process?	Set to **y** to monitor the status of the Cisco CallManager process. The default is y.
Threshold - Maximum CPU for CallManager	Specify the maximum amount of CPU usage for the Cisco CallManager process that can occur before an event is raised. The default is 80%.
Monitor other Cisco processes?	Set to **y** to monitor the status of other Cisco processes. The default is n.
Threshold - Maximum CPU for other processes?	Specify the maximum amount CPU usage for other Cisco processes that can occur before an event is raised. The default is 20%.

CCM_DeviceStatus

Use this Knowledge Script to monitor the status of key devices within a cluster. The possible statuses are:

- **Registered**. This status indicates the device is available
- **Unregistered**. This status indicates a device that was previously registered with CallManager has become unregistered. This status may be generated as part of a normal unregistration event, or can be due to another reason such as loss of keepalives.
- **Rejected**. This status indicates CallManager has rejected the registration for the device. This script detects this status only if the device was at one time registered to the CallManager but a subsequent registration attempt was rejected.
- **Unknown**. This status indicates the device has not been registered to any CallManagers in the cluster for a long time, or the device was added to a CallManager but never registered, or the CallManager RIS service is not operational.

Note
Phones that are added while this script is running will not be monitored.

The first time you run this script, it builds a device list from the criteria you have selected. At each subsequent interval, the script checks the status of these devices. If the number or percentage of these devices that are registered does not meet the threshold you define, an event is raised. The device list is not rebuilt each time you run this script. Therefore, if you add a new device, delete a device, or change device details, the changes will *not* be picked up by this script unless you stop it and then restart it. If you delete a device, the status will change to "Unknown," but the device will remain in the list until you stop and restart the script.

If you enter multiple selection criteria and the selections find the same device or devices, there will be duplicate entries in the list of devices to be monitored. This is working as designed — if you select by directory numbers, and a device has more than one directory number, you will get duplicate entries for that device.

Different *Select By* choices will build different lists of devices to be monitored even if you select the same *Device Type*. For example, if you select *DeviceName*, the list will contain all of the directory numbers for each device with that device type. If you select *DirectoryNumber*, each row in the list will contain only a single directory number. If a device has multiple directory numbers, that device will be listed multiple times.

Tip
This script uses several COM modules. There is a one-time cost of about 7-10M of memory and CPU usage of around 30-40% the first time the script is run.

Prerequisite

This script relies on the CallManager RIS (Real-Time Information Server) function to be working properly. If this function is not working on all the CallManagers in a cluster, this script may not generate accurate results. Verify the Cisco Database Layer Monitor and the Cisco RIS Data Collector services are running on all the CallManagers in the clusters.

Cisco has documented the following for CallManager:

The Real-Time Information Server (RIS) collects, distributes, and maintains real-time Cisco CallManager information and provides an interface through which the Cisco RIS Data Collector service and the SNMP Agent retrieve that information. One RIS exists on each node that contains the Cisco CallManager service. The Cisco RIS Data Collector service provides an interface for applications, such as Cisco CallManager Serviceability and the Cisco CallManager Administration, to retrieve information that is stored in all RIS nodes in the cluster.

- Cisco recommends the Cisco RIS Data Collector service reside on every server in the Cisco CallManager cluster.
- Cisco RIS Data Collector service requires the Cisco Database Layer Monitor service.

Examples of Using CCM_DeviceStatus

If you use centralized processing, you would benefit from using this script. You could monitor a group of devices at the remote site and then raise an event if a certain number of those devices were not registered.

In a second scenario, you could verify the phones in public places (such as conference rooms) have not been taken off the network. Many times, employees will use a public port for their laptops and forget to put the phone back online.

You can also use this script for troubleshooting. For example, you could retrieve the IP address of all the devices with a certain directory number.

Resource Object

CCM Publisher

Default Schedule

By default, this script runs every one minute.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold not met?	Set to **y** to raise an event if the threshold is not met. The default is y. The detailed message for the event will contain the following information about each device that is not registered: • Device Name • Description • Directory number(s) • IP address (if available) • Status • CallManager node where device was registered (if available) • Model • Device Pool (if available) • Calling Search Space (if available) For more information, see "Examples of Using CCM_DeviceStatus" on page 832.

Parameter	How to Set It
Collect data?	Set to **y** to collect data for graphs and charts. The default is n. The data collected is the number of devices that are being monitored and the number of those devices that are registered.
Event severity when threshold is not met	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is not met. The default is 10.
Device to monitor	Select the type of devices to monitor. Valid values are: • Phone (the default) • MGCP_GatewayDevice • CtiRoutePoint • VoiceMailPort • ConferenceBridge • MusicOnHoldDevice • MediaTerminationPoint
Select by	Choose the type of the selection criteria to be used to get the list of devices to monitor. Note that some criteria may not make sense for every device type. For example, you would not want to select by Directory Numbers if the Device Type is Conference Bridges. Valid values are: • DeviceName (the default) • DirectoryNumber • Description • DevicePool • CallingSearchSpace
Selection criteria	Enter the selection criteria for the devices to be monitored. You can specify the actual item or you can specify a pattern by using the * wildcard. For example, to monitor all the devices with device names that begin with SEP, enter `SEP*`. The default is *, which Indicates you want to monitor all devices. You can enter multiple items by separating each item with a comma. For example: `SEP0009A*,SEP0009B*` The items must be the same type as the *Select By* parameter. So if *Select By* is **Device Name**, the items must be device names or patterns. If *Select By* is **Directory Number**, the items must be directory numbers or patterns. **Note** If you enter a file path in *Full path to file with list of selection criteria*, ignore this parameter.
Full path to file with list of selection criteria	Enter the full path to a file on the agent computer containing a list of the selection criteria. The file should contain the selection criteria on one or more lines. Each line can have multiple items, separated by commas. For example: • `SEP0009A*,SEP0009B*` • `SEP999999994000,SEP999999994001` • `SEP00044*` The items must be the same type as the *Select By* parameter. So if *Select By* is **Device Name**, the items must be device names or patterns. If *Select By* is **Directory Number**, the items must be directory numbers or patterns. **Note** If you enter a file path, ignore the *Selection Criteria* parameter.

Parameter	How to Set It
Maximum number of devices to monitor	Enter the maximum number of devices to be monitored. Only this number of devices will be monitored even if the selection criterion returns more than this number. Enter a number between 1 and 250. The default is 100 devices. **Note** If the selection criterion does return more devices than the maximum number of devices to monitor, this script generates an event issued warning that this situation has occurred.
Raise event with current status?	Enter **y** to generate an informational event containing the current status of the devices selected the first time this script runs. The default is y. The following details will be returned about each device: • Device Name • Description • Directory number(s) • IP address (if available) • Status • CallManager node where device is\was registered (if available) • Model • Special firmware load • Device Pool (if available) • Calling Search Space (if available) If you set this parameter to y, the first time the script is run an informational event will be generated containing the current status and details of all the monitored devices. The details of this informational event can be formatted in either XML or csv.
Format status event in XML?	Set to **y** to format the informational event containing the current status in XML. The default is y. If you use XML for the event, it will not be sent to any Actions that are defined for the script. If you want this information sent to an Action, set this parameter to n. The detailed message will then be formatted in .csv.
Threshold type	Select whether you want to monitor for a **Percentage** threshold or a **Number** threshold. The default is Percentage.
Threshold - Minimum % registered key devices	Specify the minimum percentage of devices that must have a status of "Registered" before an event is raised. The default is 75%.
Threshold - Minimum # registered key devices	Specify the minimum number of devices that must have a status of "Registered" before an event is raised. The default is 0 devices.
Event severity when key devices cross threshold and then return	Set the severity, from 1 to 40, of an event that is raised when the number or percent of key devices registered was previously below the threshold but now is within acceptable limits. Enter **0** if you do not want to raise an event. The default is 20.

Event Messages for CCM_DeviceStatus

Following are common error messages, accompanied by an explanation, a likely cause, and any operator action that may be needed.

Internal error encountered.

Explanation: An unrecoverable error was encountered. See the detailed event message for details about the error.

Likely cause: In most cases this message Indicates a COM interface was not available, either because the COM object has not been installed or is not registered.

Operator action: Verify the `dblx.dll` and `risx.dll` are installed and registered on the CallManager computer.

Initial device status.

Explanation: "y" was entered for the *Generate an event with the initial status* parameter. See the detailed event message for the status.

Likely Cause: See explanation.

Operator Action: No action is required.

 # key devices registered low.

Explanation: The number of devices you have selected to be monitored that have a status of "Registered" does not meet the threshold. See the detailed event message for a list of the devices that are not "Registered."

Likely Cause: If one or two devices are unavailable, it probably means someone has unplugged them from the network. If a large number of devices is unavailable, either there is a network problem or a failover may be in progress.

Operator Action: Verify the devices are plugged into the network and are operational. In the case of a large number of devices becoming unavailable, check to see whether a failover has occurred. In the case of a failover, the devices should get re-registered to the backup CallManager and should become available again. If there is a network problem, contact the network administrator.

% key devices registered low.

Explanation: The percentage of devices you have selected to be monitored that have a status of "Registered" does not meet the threshold. See the detailed event message for a list of the devices that are not registered.

Likely Causes: If one or two devices are unavailable, it probably means someone has unplugged them from the network. If a large number of devices are unavailable, either there is a network problem or a failover may be in progress.

Operator Action: Verify the devices are plugged into the network and are operational. In the case of a large number of devices becoming unavailable, check to see whether a failover has occurred. In the case of a failover, the devices should get re-registered to the backup CallManager and should become available again. If there is a network problem, contact the network administrator.

Syntax error: nothing selected.

Explanation: You must enter input into either the *Selection Criteria* or *File path containing selection criteria* parameter

Likely Cause: All selection parameters are empty.

Operator Action: Enter input into at least one of the selection parameters.

Unable to access device file.

Explanation: The file name entered could not be read. Either the path is inaccessible from the AppManager agent or the file does not exist.

Likely Cause: In most cases this message Indicates the file does not exist.

Operator Action: Verify the file exists and the path is accessible from the AppManager agent.

No devices to monitor.

Explanation: There were no devices found that match the selection criteria entered.

Likely Cause: See explanation.

Operator Action: Change the selection criteria.

Not all devices monitored.

Explanation: The number of devices found that match the selection criteria entered is greater than the maximum number of devices to be monitored. Only the maximum number of devices will be monitored.

Likely Cause: See explanation.

Operator Action: None, if the actual devices that are being monitored meet your objective. If not, change the selection criteria if possible so that a smaller list is returned from the selection.

Some devices not found.

Explanation: Multiple selection criteria were entered and one of the selection criteria did not find any devices.

Likely Cause: Most likely, the selection criteria are being read from a file, which contains one or more selection items or patterns that did not find a match. For example, if the file contains

```
SEP000ABD123,SEP000ABD124
SEP000ADD125,SEP000ABD126
```

and `SEP000ADD125` does not exist, you will get this warning message and only three devices will be monitored.

Operator Action: None, if the actual devices that are being monitored meet your objective. If not, change or remove the selection criterion that is not returning any devices.

CCM_EventLog

Use this Knowledge Script to monitor event log entries from Cisco CallManager during the past *n* hours. This script raises an event if the log contains the entries you identify.

Example of Using this Script

Cisco CallManager records events to the Windows Application Log under the source of the CallManager process that created the event. For example, a TFTP error is recorded under "Cisco Tftp." However, monitoring the Application Log is a time-consuming process, rendering the Application Log a diagnostic tool used only long after a problem occurs.

Using the CCM_EventLog Knowledge Script to periodically filter the Application Log, you can easily search for events that meet the criteria you specify, such as *Event Source=Cisco CallManager service name* or *Event Category=Error*. AppManager then raises an event with a description of the CallManager-related event.

Searching too many records can be CPU and memory intensive.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event for log entries?	Set to **y** to raise an event when the log contains entries for which you have filtered. The default is y.
Collect data?	Set to **y** to collect data about log entries for charts and graphs. The default is n.
Separate data?	Set to **y** to separate events entries from different log files into different data streams. If set to n, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. The default is n. For example, if you are monitoring both the System and Application logs, you may want to set this parameter to **y** so that events in the System log are tracked separately from events in the Application log.
Log source	Specify the event log you want to monitor. You can specify multiple event logs, separated by commas. For example: `System,Application`. The default is Application.
Type: Error	Set to **y** to monitor for error events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for *Collect data*. The default is y.

Parameter	How to Set It
Type: Warning	Set to **y** to monitor for warning events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for *Collect data*. The default is y.
Type: Information	Set to **y** to monitor for information events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for *Collect data*. The default is n.
Type: Success Audit	Set to **y** to monitor for success audit events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for *Collect data*. The default is n.
Type: Failure Audit	Set to **y** to monitor for failure audit events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for *Collect data*. The default is n.
Instructions for filters: To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log. The search string can contain criteria used to include entries, exclude entries, or both.· • Separate include and exclude criteria with a colon (:). For example, `net:logon`. • Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ`. • If you are specifying only include criteria, the colon is not necessary. For example, `SQL`. • If you are specifying only exclude criteria, start the search string with a colon. For example, `:defragmentation,cleanup`.	
Event source filter	Specify one or more text strings to look for; separate multiple strings with commas. For example: `NTDS KCC,NTDS General`
Event category filter	Specify one or more text strings to look for; separate multiple strings with commas.
Event ID filter	Specify a single event ID or a range of event IDs; separate multiple entries by commas. For example: `1094,1404-1463`
Event user filter	Specify a single or multiple user names to look for; separate multiple entries by commas. For example: `Pat,Chris,Alex`
Computer filter	Specify a single or multiple computer names to look for; separate multiple entries by commas. For example: `SHASTA,MARS`
Event description filter	Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods; separate multiple entries with commas. For example: `data loss during system failures,corrupt indices,Inter-Site Transport objects failed`
Maximum number of entries per event report	Specify the maximum number of Application log events that can be returned in each event report. For example, if this value is set to 30 and 67 Application log events are found, three event reports are raised: two reports containing 30 events and one report containing seven events. The default is 30. The Message column on the Events tab displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.
Event severity for log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event. You may want to adjust the severity depending on the types of events for which you are checking. The default is 8.

CCM_FXOPorts

Use this Knowledge Script to monitor the number of active and in-service FXO (foreign exchange office) ports for this CallManager. This script raises an event if a monitored value exceeds or falls below the threshold you set.

The ports or channels you monitor can be on one or more MGCP gateways.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if either threshold is breached. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of a breached threshold. The default is 15.
Threshold - Maximum active FXO ports	Specify the maximum number of FXO ports that can be active before an event is generated. The default is 10 ports.
Threshold - Minimum in-service FXO ports	Specify the minimum number of FXO ports that can be in service before an event is generated. The default is 0 ports.

CCM_FXSPorts

Use this Knowledge Script to monitor the number of active and in-service FXS (foreign exchange station) ports for this CallManager. This script raises an event a monitored value exceeds or falls below the threshold you set.

The ports or channels you monitor can be on one or more MGCP gateways.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if either threshold is breached. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of a breached threshold. The default is 15.
Threshold - Maximum active FXS ports	Specify the maximum number of FXS ports that can be active before an event is generated. The default is 10 ports.
Threshold - Minimum in-service FXS ports	Specify the minimum number of FXS ports that can be in service before an event is generated. The default is 0 ports.

CCM_HealthCheck

Use this Knowledge Script to monitor the status of Cisco CallManager services. This script automatically starts any down service when *Auto-start monitored services* is set to **y**.

This script collects the data used by the Report_ServicesAvailability Knowledge Script.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every one minute.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to **y** to enable this script to collect data for reports and graphs. The default is y.
Auto-start monitored service(s)?	Set to **y** to automatically start any of the services you choose to monitor. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager has not been set to restart the service. The default is 18.
Event severity when service does not exist	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service does not exist. The default is 15.
Event severity when service is paused	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service is in a paused state. The default is 20. Some services enter a paused state when the system is low on CPU or memory resources. Enter **0** when you do not want to raise an event for this situation.
Monitor Cisco CallManager service?	Set to **y** to monitor the status of Cisco CallManager. The default is y.
Monitor Cisco Database Layer Monitor service?	Set to **y** to monitor the status of Cisco Database Layer Monitor. The default is y.
Monitor Cisco TFTP service?	Set to **y** to monitor the status of Cisco TFTP. The default is y.
Monitor Cisco IP Voice Media Streaming App service?	Set to **y** to monitor the status of Cisco IP Voice Media Streaming App. The default is n.

Parameter	How to Set It
Monitor Cisco Messaging Interface service?	Set to **y** to monitor the status of Cisco Messaging Interface. The default is n.
Monitor Cisco Telephony Call Dispatcher service?	Set to **y** to monitor the status of Cisco Telephony Call Dispatcher. The default is y.
Monitor DC Directory Server service?	Set to **y** to monitor the status of the DC Directory Server service. The default is y.
Monitor Cisco SNMP Data Collector service? (for CallManager 3.0 only services)	Set to **y** to monitor the status of Cisco SNMP Data Collector. The default is n.
Monitor Cisco CTI Manager service?	Set to **y** to monitor the status of Cisco CTI Manager (for CallManager 3.1 and later). The default is n.
Monitor Cisco Extension Mobility Logout service?	Set to **y** to monitor the status of Cisco Extension Mobility Logout (for CallManager 3.1 and later). The default is n.
Monitor Cisco MOH Audio Translator service?	Set to **y** to monitor the status of Cisco MOH Audio Translator (for CallManager 3.1 and later). The default is n.
Monitor Cisco RIS Data Collector service?	Set to **y** to monitor the status of Cisco RIS Data Collector (for CallManager 3.1 and later). The default is n.

CCM_HeartBeat

Use this Knowledge Script to monitor the CallManager heartbeat. This script raises an event if the heartbeat stops or falls below the specified threshold. A low heartbeat Indicates the CallManager service was stopped and then restarted.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every one minute.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if heartbeat stops or falls below the threshold?	Set to **y** to raise an event when the heartbeat stops or falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about the heartbeat for reports and graphs. The default is n.
Threshold - Minimum heartbeat	Specify the minimum heartbeat count that can be detected before an event is raised. The default is 500.
Event severity when heartbeat falls below the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the heartbeat fell below the threshold. The default is 20.
Event severity when heartbeat stops	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the heartbeat stopped. The default is 10.

CCM_MemByProcess

Use this Knowledge Script to monitor working set memory use for individual CallManager processes, and the total working set memory use for all monitored CallManager processes. This script raises an event if working set memory use exceeds the threshold. If a process cannot be found, no events are generated.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data for memory use by all monitored processes?	Set to **y** to collect data for the total amount of memory being used by all the monitored processes. The default is y.
Threshold - Maximum memory use for all monitored processes	Specify the maximum amount of memory that can be used by all the monitored processes before an event is raised. The default is 512000 KB.
Event severity when total memory use exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which memory use for all monitored processes exceeds the threshold. Enter **0** if you do not want to raise an event. The default is 15.
Collect data for memory use by individual processes?	Set to **y** to collect data for the amount of memory being used by each monitored process.
Event severity when individual memory use exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which memory use for individual processes exceeds the threshold. Enter **0** if you do not want to raise an event. The default is 15.
Monitor the CallManager process?	Set to **y** to monitor memory usage of the Cisco CallManager process. The default is y.
Threshold - Maximum memory use for the CallManager process	Specify the maximum amount of memory that can be used by the Cisco CallManager process before an event is raised. The default is 200000 KB.
Monitor the DC Directory process?	Set to **y** to monitor memory usage of the DC Directory process. The default is y.
Threshold - Maximum memory use for the DC Directory process	Specify the maximum amount of memory that can be used by the DC Directory processes before an event is raised. The default is 100000 KB.
Monitor the CTI Manager process?	Set to **y** to monitor memory usage of the CTI Manager process. The default is y.
Threshold - Maximum memory use for the CTI Manager process	Specify the maximum amount of memory that can be used by the CTI Manager process before an event is raised. The default is 50000 KB.
Monitor the Cisco TFTP process?	Set to **y** to monitor memory usage of the Cisco TFTP process. The default is y.

Parameter	How to Set It
Threshold - Maximum memory use for the Cisco TFTP process	Specify the maximum amount of memory that can be used by the Cisco TFTP process before an event is raised. The default is 50000 KB.
Monitor the Database Layer process?	Set to **y** to monitor memory usage of the Database Layer process (Aupair). The default is y.
Threshold - Maximum memory use for the Database Layer process	Specify the maximum amount of memory that can be used by the Database Layer process before an event is raised. The default is 50000 KB.
Monitor the Telephony Call Dispatcher process?	Set to **y** to monitor memory usage of the Telephony Call Dispatcher process. The default is y.
Threshold - Maximum memory use for the Telephony Call Dispatcher process	Specify the maximum amount of memory that can be used by the Telephony Call Dispatcher process before an event is raised. The default is 50000 KB.
Monitor the CDR Insert process?	Set to **y** to monitor memory usage of the CDR Insert process. The default is n.
Threshold - Maximum memory use for the CDR Insert process	Specify the maximum amount of memory that can be used by the CDR Insert process before an event is raised. The default is 75000 KB.
Monitor the Messaging Interface process?	Set to **y** to monitor memory usage of the Messaging Interface process. The default is n.
Threshold - Maximum memory use for the Messaging Interface process	Specify the maximum amount of memory that can be used by the Messaging Interface process before an event is raised. The default is 50000 KB.
Monitor the Extension Mobility process?	Set to **y** to monitor memory usage of the Extension Mobility process. The default is n.
Threshold - Maximum memory use for the Extension Mobility process	Specify the maximum amount of memory that can be used by the Extension Mobility process before an event is raised. The default is 50000 KB.
Monitor the MOH Audio Translator process?	Set to **y** to monitor memory usage of the MOH (Music On Hold) Audio Translator process. The default is n.
Threshold - Maximum memory use for the MOH Audio Translator process	Specify the maximum amount of memory that can be used by the MOH Audio Translator process before an event is raised. The default is 50000 KB.
Monitor the RIS Data Collector process?	Set to **y** to monitor memory usage of the RIS (Real-Time Information Server) Data Collector process. The default is n.
Threshold - Maximum memory use for the RIS Data Collector process	Specify the maximum amount of memory that can be used by the RIS Data Collector process before an event is raised. The default is 50000 KB.
Monitor the IP Voice Streaming Media process?	Set to **y** to monitor memory usage of the IP Voice Streaming Media process. The default is n.
Threshold - Maximum memory use for the IP Voice Streaming Media process	Specify the maximum amount of memory that can be used by the IP Voice Streaming Media process before an event is raised. The default is 50000 KB.

CCM_MemoryHigh

Use this Knowledge Script to monitor the memory that application processes are consuming. This script checks the memory used by each process individually, and the total memory used by all processes. If a process is not found, the script assumes that the process is not running, and reports zero as the memory result.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if one of the thresholds is exceeded. The default is y.
Collect data?	Set to **y** to collect data about memory usage for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.
Monitor the Cisco CallManager process?	Set to **y** to monitor the Cisco CallManager process. The default is y.
Threshold - Maximum memory usage for CallManager process	Specify the maximum memory usage by the CallManager process that can occur before an event is raised. The default is 200000 KB.
Threshold - Maximum memory pool usage for CallManager process	Specify the maximum memory pool usage by the CallManager process that can occur before an event is raised. The default is 5000 KB.
Monitor other Cisco processes?	Set to **y** to monitor other Cisco processes. The default is n.
Threshold - Maximum memory usage for other Cisco processes	Specify the maximum memory usage by other Cisco processes that can occur before an event is raised. The default is 25000 KB.
Threshold - Maximum memory pool use for other Cisco processes	Specify the maximum memory pool usage by other Cisco processes that can occur before an event is raised. The default is 5000 KB.

CCM_MOHUnavailable

Music on Hold (MOH) resources are provided by software-based MOH servers that register with CallManager. MOH servers are configured through CallManager Administration. Each MOH server is capable of supplying up to 500 Unicast output streams and 204 Multicast streams simultaneously, and can be configured for up to 51 different audio sources.

Use this Knowledge Script to monitor the number of times that an attempt was made to allocate an MOH resource when either every available connection on all MOH servers was active, or when no MOH servers were registered.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of out-of-resource instances exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about out-of-resource instances for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of out-of-resource instances exceeds the threshold. The default is 10.
Threshold - Maximum out-of-resource instances	Specify the maximum number of out-of-resource instances that can occur before an event is raised. The default is 0.

CCM_PhoneCheck

Use this Knowledge Script to monitor your CallManager for new and missing phones. With each iteration of the job, this script creates a list of the phones registered to the CallManager, and then compares the latest list information with the information from the previous list. You can determine the frequency with which this script runs from the **Schedule** tab.

Notes

- This script does not return information about H.323 devices.
- The list is sorted by the Description, not the Device Name, of the phone that you configured in CallManager.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Script Options	
Name for current phone list	Provide a name for the current list of new or missing phones. The default is `NQCurrentPhoneList`.
Name for global phone list	Provide a name for the global list of new or missing phones. The default is `NQGlobalPhoneList`.
Monitor New and Missing Phones	
Event Notification	
Raise event if new phones are found?	Select **Yes** to raise an event if new phones are found since the last time you ran the script. The default is Yes.
Event severity when new phones are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which new phones are found. The default is 30.
Raise event if phones are missing?	Select **Yes** to raise an event if any phones are missing since the last time you ran the script. The default is Yes.
Event severity when phones are missing	Set the severity level, from 1 to 40, to indicate the importance of an event in which phones are missing. The default is 15.

CCM_PhoneInventory

Use this Knowledge Script to take an inventory of phones based on specified search criteria and to write the inventory results to a file. Unless you specify a UNC path, *servername**sharename**directoryname**filename*, the results file is written on the CallManager Publisher computer where the NetIQ agent is running.

Monitoring Phone Status

You can determine the status (registered or deregistered) of CallManager phones for active CallManager 4.x clusters and for CallManager 4.x clusters on which failover has occurred. Failover occurs when CallManager status changes from Primary to Backup.

For active CallManager clusters

In this scenario, use the phone deregistration support provided by the CiscoCM_4x_PhoneDeregistrations Knowledge Script from the AppManager for Cisco Unified CallManager module. By using this script, you can determine which phones have deregistered and maintain a history of phone deregistrations in the Cisco CM supplemental database.

AppManager for Cisco Unified CallManager provides limited support for monitoring phone deregistrations on CallManager 4.x clusters. For more information, see the *AppManager for Cisco Unified CallManager Management Guide*.

For CallManagers that have failed over

CallManagers that fail over contain only a list of phones that have registered since failover occurred. They do not provide a list of phones that deregistered as a result of failover. Use the CCM_PhoneInventory Knowledge Script to determine which phones have deregistered. Use the *Monitor for new/missing phone registrations?* parameter to monitor for phone registrations that are missing since the last time this script was run.

To determine whether failover has occurred, use the CCM_RoleStatus or LossOfHardwarePhones Knowledge Script.

Resource Object

CCM Publisher

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Script Options	
Collect data?	Select **Yes** to collect data about the number of configured and registered phones for reports and graphs. The default is unselected.

Parameter	How to Set It
CallManager database username	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Monitor for new/missing phone registrations?	Select **Yes** to monitor for phone registrations that are new or missing since the last time this script was run. The default is unselected.
Search Options	
Select by	Choose the type of the selection criteria that you want to use to create the list of phones. • Name (the default) • DirectoryNumber • Description • DevicePool • CallingSearchSpace • Partition • Subnet. If you select this option, you must enter the subnet address in the *Selection criteria* parameter. Use the following syntax: `172.16.10.0/20`. • SubnetFilepath. If you select this option, in the *Selection criteria* parameter, enter the UNC or full path to a file on the agent computer that contains a list of subnet specifications.
Selection criteria	Provide the selection criteria for the phones to be listed. You can specify the actual item or you can specify a pattern by using the * wildcard. For example, to monitor all the phones with device names that begin with SEP, enter `SEP*`. You can enter multiple items by separating each item with a comma. For example: `SEP0009A*,SEP0009B*` The items you enter must be of the same type as the *Select by* parameter. So if *Select by* is **Name**, the items you enter must be device names or patterns. If *Select by* is **Directory Number**, the items you enter must be directory numbers or patterns.
Result File Options	

Parameter	How to Set It
Write details to result file?	Select **Yes** to write the details about each phone to the result file specified in the *Result file name* parameter. The default is Yes. The following details about each phone will be returned in a `.csv` file: • Name • Description • Directory number • Partition (if available) • Model • Device Pool (if available) • Calling Search Space (if available) • Location • IP address (if available) • CallManager node where device is\was registered (if available) • Status • Status Time
Result file name	Provide the full path or a UNC path to a location on the agent computer where the inventory `.csv` file should be written. The default path is `c:\Program Files\NetIQ\Temp\NetIQ_Debug\PhoneInventory.csv`
Write phone registration change details to a second result file?	Select **Yes** to write the details about new or missing registrations to the result file specified in the *Phone registration changes file name* parameter. The default is Yes.
Phone registration changes file name	Provide the full path or a UNC path to a location on the agent computer where the registration changes `.csv` file should be written. The default path is `c:\Program Files\NetIQ\Temp\NetIQ_Debug\PhoneInventoryComparison.csv`
List only phone with status of	Use this parameter to limit the phones listed in the results file to only those whose status is one of the following: • Any (the default) • Not Registered • Registered • Unregistered • Rejected • Unknown **Note** Setting this parameter to a value of **Not Registered** will list those phones with a status of **Unregistered**, **Rejected**, and **Unknown**.
Order by	Select **Name** to display the contents of the results file in order by the phone name. The default is Name. Select **DirectoryNumber** to display the contents of the results file in order by directory numbers.
Threshold	
Threshold type	Select whether you want to monitor for **Percentage** or **Number** thresholds. The default is Percentage.
Threshold - Minimum % phones registered	Specify the minimum percentage of phones that must have a status of Registered before an event is raised. The default is 75%.

Parameter	How to Set It
Threshold - Minimum # phones registered	Specify the minimum number of phones that must have a status of Registered before an event is raised. The default is 0 phones.
Events	
Raise event if threshold is exceeded?	Select **Yes** to raise an event when a threshold is exceeded. The default is Yes.
Raise informational event when inventory completes?	Select **Yes** to raise an informational event when the inventory has completed. The default is Yes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Event severity when failures occur	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a failure occurred, such as an inability to write to the file or access the database. The default is 15.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the results file returns no data. The default is 30.

Event Messages for CCM_PhoneInventory

The following are common event messages, accompanied by an explanation, a likely cause, and any operator action that may be needed.

PhoneInventory: x Configured and y Registered

Explanation: This message is returned when the inventory completes.

Likely causes: The script ran successfully.

Operator action: No action required.

 # registered phones is low

Explanation: The number of phones in the inventory that have a status of Registered does not meet the threshold.

Likely causes: If one or two phones are unavailable, it probably means that someone has unplugged them from the network. If many phones are unavailable, either there is a network problem or a failover may be in progress.

Operator action: Verify that the phones are plugged into the network and are operational. If many phones are unavailable, check to see whether a failover has occurred. If a failover has occurred, the phones should get re-registered to the backup CallManager and should become available again. If there is a network problem, contact the network administrator.

% registered phones is low

Explanation: The percentage of phones in the inventory that have a status of Registered does not meet the threshold.

Likely causes: If one or two phones are unavailable, it probably means that someone has unplugged them from the network. If many phones are unavailable, either there is a network problem or a failover may be in progress.

Operator action: Verify that the phones are plugged into the network and are operational. If many phones are unavailable, check to see whether a failover has occurred. If a failover has occurred, the phones should get re-registered to the backup CallManager and should become available again. If there is a network problem, contact the network administrator.

Syntax error: <reason>

Explanation: One or more parameters entered are invalid. See the detailed event message for details about the error.

Likely causes: An invalid parameter or combination of parameters were entered.

Operator action: Fix the invalid parameter and run the script again.

Unable to access result file.

Explanation: The file name entered could not be accessed.

Likely causes: The path is inaccessible from the NetIQ agent, *or* the NetIQ agent does not have the proper permissions to access the file, *or* the file is in use by another process.

Operator action: Verify that the file is not use by another process and the path is accessible from the NetIQ agent. If you are trying to write to a network share, you may need to change the netiqmc service to not run as the LocalSystem account. In most cases, this account does not have the necessary permissions to write to a network drive.

Error encountered getting password.

Explanation: A database user name was entered and errors were encountered while trying to retrieve the password for this user name from the NetIQ AppManager Security Manager.

Likely causes: In most cases, this message Indicates the user name has not been properly entered in AppManager Security Manager.

Operator action: Verify that the user name has been properly entered in AppManager Security Manager.

Incorrect managed object version.

Explanation: The NetIQ CallManager managed object (`qccma4.dll`) is not at the correct level to run this script.

Likely causes: The NetIQ agent on the CallManager server being monitored is not at the latest level.

Operator action: Upgrade the NetIQ agent to the latest level.

Database operation failed.

Explanation: An error was encountered executing a SQL query.

Likely causes: In most cases this message Indicates the NetIQ agent does not have the proper authority to execute the query. Another reason could be that the SQL query timed out because the SQL server was too busy. The detailed message should contain the reason that the SQL query failed.

Operator action: If a timeout occurred, try the query at a time when the SQL server is not so busy. If using a user name and password, verify that the user name has access to the CallManager configuration database. If using Windows authentication (blank user name), verify that the `netiqmc` process is running with the correct permissions to access the database.

Internal error encountered.

Explanation: An unrecoverable error was encountered. See the detailed event message for details about the error.

Likely causes: In most cases this message Indicates a COM interface was not available, either because the COM object has not been installed or is not registered.

Operator action: Verify that the NetIQ CallManager managed object (`qccma4.dll`) is installed and registered on the CallManager server.

CCM_PRIChannels

Use this Knowledge Script to monitor the number of active and in-service PRI (primary rate interface) channels for this CallManager. This script raises an event if a monitored value exceeds or falls below the threshold you set.

The ports or channels you monitor can be on one or more MGCP gateways.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if either threshold is breached. The default is y.
Collect data?	Set to **y** to collect data about PRI channels for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls. The default is y.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is breached. The default is 15.
Threshold - Maximum active PRI channels	Specify the maximum number of PRI channels that can be active before an event is raised. The default is 10 channels.
Threshold - Minimum PRI spans in service	Specify the minimum number of PRI spans that can be in service before an event is raised. The default is 0 channels.

CCM_Replication

Use this Knowledge Script to query for failed actions in the distribution, snapshot, and logreader history tables of the replication agents on the CallManager Publisher.

Replication allows you to keep copies of the same data on multiple sites. The Publisher is the source of the replication. The Publisher defines an article for each table or other database object to be used as a replication source. One or more related articles from the same database are organized into a *publication*. A publication is a convenient way to group together related data that you want to replicate.

The Subscriber receives the replication data from the Publisher. The Subscriber defines a *subscription* to a particular publication. The subscription specifies when the Subscriber receives the publication from the Publisher, and maps the articles to tables and other database objects in the Subscriber.

Cisco CallManager uses two types of replication:

Snapshot Replication

Snapshot replication copies data or database objects exactly as they exist at the time of replication. Snapshot publications are typically defined to occur on a scheduled basis, however, the publication is sent to the Subscriber only if the latest publication reflects a difference from the previous publication. The Subscriber contains copies of the published articles, as they existed at the time of the last snapshot. Snapshot replication is typically used when the source data is relatively static, or when the Subscribers can be slightly out of date, or if the amount of data to replicate is small.

Transactional Replication

In a transactional replication, Subscribers are first synchronized with the Publisher (typically by using a snapshot), and then, as the publication data is modified, the transactions are captured and sent to the Subscribers. Transactional integrity is maintained across the Subscribers by having all modifications made at the Publisher and then replicated to the Subscribers. Transactional replication is typically used when data must be replicated as it is modified, you must preserve the transactions, and the Publishers and Subscribers are reliably and frequently connected through the network.

Database replication is accomplished through the use of several replication agents, processes that perform specific replication tasks. CallManager uses three replication agents: snapshot agent, log reader agent, and distribution agent.

To begin transactional replication, the Subscriber needs an initial snapshot of the entire database. The *snapshot agent* on the Publisher collects the information for database snapshots. The snapshot agents takes a snapshot only if a Subscriber becomes out of sync with the Publisher, or if the subscription was re-initialized. If the Subscriber does not need a snapshot, the snapshot agent does nothing when it runs on its schedule.

The *log reader agent* is responsible for moving any changes made to the Publisher database to the distribution database. For each Subscriber, a *distribution agent* is responsible for taking information from the distribution database and moving it to the appropriate Subscriber.

Note
This script assumes that the distribution database on the CallManager Publisher has not been renamed to something other than “distribution,” which is the name assigned when CallManager installed the database.

Resource Object

CCM Publisher

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
On first run, hours to go back	Specify the number of hours of previous replication agent history to check the first time you run this script. For instance, if you enter 24, the first time you run this script it will check actions made by the agents in the last 24 hours. On subsequent runs, it will check only agent actions that have occurred during the interval. The default is 1 hour. **Note** Using a high "hours to go back" time may cause this script to be CPU-intensive on its first run, depending on the number of database entries being retrieved from the server.
Distribution database username	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum failed actions by any agent	Specify the maximum number of failed actions that can have occurred during the interval for any of the agents. If the number of failed actions is greater than the threshold that you set, an event is raised. The default is 0.
Raise informational event with agent history?	Set to **y** to raise an informational event containing the last 10 actions that occurred during the interval for each replication agent. The default is y.
Raise informational event if snapshot generated?	Set to **y** to raise an informational event if, during the interval, the snapshot agent on the CallManager Publisher has generated any replication snapshots. The default is y.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold has been exceeded. The default is 5.
Event severity for informational messages	Set the severity level, from 1 to 40, to indicate the importance of an informational event message. The default is 30.

Parameter	How to Set It
Event format	Select the format in which you want to receive the informational event: CSV, XML, or both. If you select **Both**, the CSV (comma separated value) event is collapsed under the XML event. To access the CSV event, turn off **Collapse duplicate events into a single event** on the Advanced tab before running this script. **Notes** • Events formatted in XML are not forwarded to an Action script (if you selected to initiate an Action script if this script generates an event). If you select **Both**, two events are generated: one in CSV format, which is forwarded to an Action script, and one in XML format. • Error messages are formatted in plain text — this parameter does not apply to error messages.

Event Messages for CCM_Replication

Following are common event messages, accompanied by an explanation, a likely cause, and any operator action that may be needed.

 # failed replications actions high.

Explanation: The number of failed actions in one or more of the replication agent history tables exceeded the threshold.

Likely cause: One or more replication actions have failed.

Operator action: Check the detailed message, which will contain a list of the last 25 failed actions, as well as the name of the replication agent that has the failures. Forward the information to your database administrator.

Replication history.

Explanation: This is an informational message containing the last 25 actions for all the replication agents. See the detailed event message for the data.

Likely cause: This is a normal event message when *Generate informational event with agent history?* is set to "y."

Operator action: No action is required.

Replication snapshot(s) generated.

Explanation: This is an informational message created when a replication snapshot has been generated on the CallManager Publisher during the interval. See the detailed event message for information about the snapshot.

Likely cause: This is a normal event message when *Generate informational event if a replication snapshot was generated?* is set to "y."

Operator action: No action is required.

Error encountered getting password.

Explanation: A database user name was entered and errors were encountered while trying to retrieve the password for this user name from the AppManager Security Manager.

Likely cause: In most cases, this message Indicates the user name was not properly entered in the AppManager Security Manager.

Operator action: Verify that the user name has been properly entered in the AppManager Security Manager.

Incorrect managed object version.

Explanation: The AppManager CallManager managed object (`qccma4.dll`) is not at the correct level to run this script.

Likely cause: The AppManager agent on the CallManager server being monitored is not version 6.0.

Operator action: Upgrade the AppManager agent to Version 6.0 or later.

No CallManager replication agents found.

Explanation: No CallManager replication agents (snapshot, log reader, or distribution) were found when querying the distribution database on the Publisher.

Likely cause: In most cases, this message occurs when the distribution database has been renamed to something other than "distribution."

Operator action: Verify that the distribution database has not been renamed.

Database operation failed.

Explanation: An error was encountered while executing a SQL query.

Likely cause: In most cases, this message Indicates the AppManager agent does not have the proper authority to execute the query. The detailed message should contain the reason for the failure of the SQL query.

Operator action: If using a user name and password, verify that the user name has access to the distribution database. If using Windows authentication (blank user name), verify that the netiqmc process is running with the correct permissions to access the distribution database.

Internal error encountered.

Explanation: An unrecoverable error was encountered. See the detailed event message for details about the error.

Likely cause: In most cases, this message Indicates a COM interface was not available, because either the COM object is not installed or is not registered.

Operator action: Verify that the AppManager CallManager managed object (`qccma4.dll`) is installed and registered on the CallManager server.

CCM_ResetDevice

Use this Knowledge Script to reset one or more devices in order for the devices to pick up new default firmware. For example, if a new firmware load is placed on the TFTP servers, all devices using this firmware need to be reset.

To avoid resetting all the devices during peak times, schedule this script to run when the system is not busy.

This script initiates only the Reset or Restart command. It does *not* check on the success or failure of the command.

If a device is not registered with Cisco CallManager, you cannot reset or restart it. Resetting a gateway/trunk drops any in-progress calls that are using the gateway/trunk. Restarting a gateway tries to preserve the in-progress calls that are using the gateway. Other devices wait until calls are complete before restarting or resetting. Resetting or restarting an H.323 device does not physically reset or restart the device, but only re-initializes the configuration loaded by Cisco CallManager.

Note
Only an AppManager administrator should run this script.

Resource Object

CCM Publisher

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Select reset type	Select the type of reset that you want to initiate: **Reset** or **Restart**. This parameter is valid only for the Directory Number, Device Name, and Device Description patterns. The reset type is *always* Reset for the Device Type and Device Pool parameters. A Restart resets the device without shutting it down. A Reset shuts down the device and then restarts it. The default is Reset.
Directory Number pattern	Specify the directory number pattern of the devices that you want to reset. You can specify a group of directory numbers by using the % wildcard. For example, to reset all the devices with directory numbers that begin with "31," enter 31%. The reset/restart is performed only if the pattern results in 100 or fewer devices being selected.
Device Name pattern	Specify the device name pattern of the devices that you want to reset. You can specify a group of device names by using the % wildcard. For example, to reset all the devices with device names that begin with "SEP," enter SEP%. The reset/restart is performed only if the pattern results in 100 or fewer devices being selected.

Parameter	How to Set It
Device Description pattern	Specify the device description pattern of the devices that you want to reset. You can specify a group of device descriptions by using the % wildcard. For example, to reset all the devices with device descriptions that begin with "Auto," enter `Auto%`. The reset/restart is performed only if the pattern results in 100 or fewer devices being selected.
Select device type	Select the type of the device that you want to reset. All devices of that type will be reset. The default is None. Valid device types are indicated as follows: • AllPhones, which resets devices of the following types: Cisco 12 S, Cisco 12 SP, Cisco 12 SP+, Cisco 30 SP+, Cisco 30 VIP, Cisco IP Phone 7905, Cisco IP Phone 7910, Cisco IP Phone 7935, Cisco IP Phone 7940, Cisco IP Phone 7960, Cisco ATA 186, Cisco VGC Phone, Cisco VGC Virtual Phone, and H.323 Phone. • All79xxPhones, which resets devices of the following types: Cisco IP Phone 7905, Cisco IP Phone 7910, Cisco IP Phone 7935, Cisco IP Phone 7940, and Cisco IP Phone 7960. • Analog Access • Analog Access WS-X6624 • Cisco 12 S, 12 SP, and 12 SP+ • Cisco 30 SP+ and 30 VIP • Cisco IP Phone 7905, 7910, 7935, 7940, and 7960 • Cisco ATA 186 • Cisco VGC Phone and VGC Virtual Phone • Conference Bridge and Conference Bridge WS-X6608 • Digital Access, Digital Access WS-X6608, and Digital Access+ • H.323 Phone • Load Simulator • MTP and MTP WS-X6608 • MGCP Station and MGCP Trunk • VGC Gateway • 14-Button Line Expansion Module
Device pool name	Specify the name of the device pool that you want to reset. All devices in the pool will be reset.
Event severity when reset succeeds	Set the severity level of the event, from 1 to 40, to indicate the importance of an event in which the reset succeeds. The default is 25. For more information, see "Event Messages for CCM_ResetDevice" on page 861.
Event severity when warnings occur	Set the severity level of the event, from 1 to 40, to indicate the importance of the event in which warnings occurred. The default is 15.
Event severity when errors occur	Set the severity level of the event, from 1 to 40, to indicate the importance of the event in which errors occurred. The default is 5.

Event Messages for CCM_ResetDevice

Following are three common event messages, accompanied by an explanation, a likely cause, and any operator action that may be needed.

Reset issued successfully.

Explanation: The reset command was issued successfully for all selected devices. See the detailed event message for the number of devices for which the reset was issued.

Likely cause: Normal message.

Operator action: None.

Reset issued with warnings.

Explanation: Warnings were encountered while issuing the reset command for one or more of the selected devices. See the detailed event message for more information.

Likely causes: In most cases, this message Indicates one or more of the selections resulted in no devices being found to reset. Another likely cause is that too many devices were selected for reset.

Operator action: No action is required if there are no devices associated with the command. If too many devices were selected, then, if possible, use the device type or device pool parameter.

Reset issued with errors.

Explanation: Errors were encountered while issuing the reset command for one or more of the selected devices. See the detailed event message for details about the error.

Likely cause: In most cases, this message Indicates a COM interface was not available, either because the COM object has not been installed or because the COM object is not registered.

Operator action: Verify that the `dblx.dll` is installed and registered on the CallManager computer.

CCM_RestartService

Use this Knowledge Script to schedule a CallManager service to stop and then restart after a specified interval. This script raises an event when stop fails or succeeds, when restart fails or succeeds, and when the status of a service is unavailable. In addition, this script generates data streams for service availability.

Resource Object

CCM Service folder

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to **y** to collect data about CallManager services for graphs and reports. The default is n.
Wait N seconds before restarting	Set the number of seconds that you want to wait before restarting a stopped CallManager service. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the stop failed. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the restart failed. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the service is unavailable. The default is 15.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the stop succeeds. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the restart succeeds. The default is 25.
Event severity when service is paused	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service is paused. The default is 20. Some services enter a paused state when the system is low on CPU or memory resources. Enter **0** when you do not want to raise an event for this situation.
Restart Cisco CallManager service?	Set to **y** to restart Cisco CallManager. The default is y.
Restart Cisco Database Layer Monitor service?	Set to **y** to restart Cisco Database Layer Monitor. The default is y.
Restart Cisco IP Voice Media Streaming App service?	Set to **y** to restart Cisco IP Voice Media Streaming App. The default is n.
Restart Cisco Messaging Interface service?	Set to **y** to restart Cisco Messaging Interface. The default is n.
Restart Cisco SNMP Data Collector service?	Set to **y** to restart Cisco SNMP Data Collector. The default is n.

Parameter	How to Set It
Restart Cisco Telephony Call Dispatcher service?	Set to **y** to restart Cisco Telephony Call Dispatcher. The default is n.
Restart Cisco TFTP service?	Set to **y** to restart Cisco TFTP. The default is n.
Restart Cisco SNMP Data Collector service? (For CallManager 3.0 only)	Set to **y** to restart Cisco SNMP Data Collector service. The default is n.
Restart Cisco CTI Manager service? (for CallManager 3.1 only)	Set to **y** to restart Cisco CTI Manager. The default is n.
Restart Cisco Extension Mobility Logout service? (for CallManager 3.1 only)	Set to **y** to restart Cisco Extension Mobility Logout. The default is n.
Restart Cisco MOH Audio Translator service? (for CallManager 3.1 only)	Set to **y** to restart Cisco MOH Audio Translator. The default is n.
Restart Cisco RIS Data Collector service?	Set to **y** to restart Cisco RIS Data Collector. The default is n.

CCM_RoleStatus

Use this Knowledge Script to determine whether a CallManager's status is Primary or Backup. You can choose to raise an event for status transitions. A Backup is defined as any CallManager with no registered hardware or software phones.

In the event of a failover from a Primary CallManager to a Backup CallManager, you can set the **Actions** tab of this script to run Action_RunDiscoveryCiscoCallMgr. The Action script will discover CallManager resources on the backup device and, if you have configured a monitoring policy to do so, any jobs that are running on the Primary device will be transferred to the Backup CallManager.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

You can also use this script to monitor phone status. For more information, see "CCM_PhoneInventory" on page 849.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when Backup changes to Primary?	Set to **y** to raise an event when the CallManager status changes from Backup to Primary. The default is y.
Event severity when Backup changes to Primary	Set the event severity level, from 1 to 40,to indicate the importance of an event in which the status changes from Backup to Primary. The default is 15.
Raise event when Primary changes to Backup?	Set to **y** to raise an event when the CallManager status changes from Primary to Backup. The default is y.
Event severity when Primary changes to Backup	Set the event severity level, from 1 to 40,to indicate the importance of an event in which the status changes from Primary to Backup. The default is 15.
Collect data?	Set to **y** to collect data for reports and graphs. A Primary returns a value of 100; a Backup returns a value of 0. The default is n.

CCM_SecureWebPageCheck

Use this Knowledge Script to monitor accessibility to the `ccmadmin` and `ccmuser` secure Web pages, and raise an event if the Web pages cannot be accessed. This script can collect data about the availability of the Web pages and round-trip connection time. If a URL is not reachable, the detail message records the reason, such as the format of the request was invalid or the server name was not found. If the Web pages cannot be accessed, you can arrange for this script to restart the IIS server and sites that are down.

Note
This script is supported for Cisco CallManager version 4.1 or later. If you are running an earlier version, use CCM_WebPageCheck.

Resource Objects

CCM IIS Server

CCM IIS W3 SRV

CCM IIS Web Inst

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if Web page is inaccessible?	Set to **y** to raise an event if the Web page cannot be accessed. The default is y.
Collect data for up/down URL?	Set to **y** to collect data about the up and down status of the URL. If set to y, the script returns a value of 100 if the connection is up and a value of 0 if the connection is down. The default is y.
Collect data for round-trip time?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the round-trip connection time (in milliseconds). The default is n.
Monitor ccmadmin?	Set to **y** to monitor the ccmadmin Web page. The default is y.
Monitor ccmuser?	Set to **y** to monitor the ccmuser Web page. The default is y.
Username for ccmadmin	Enter the user name to use when logging on to ccmadmin. If a user name is not required, you can leave this field blank. For more information about the user name, see "CCMAdmin User Name and Password Configuration" on page 867.

Parameter	How to Set It
Treat Access Denied errors as "Up"?	When no password or user name is specified for ccmadmin, the URL check for ccmadmin will produce an "access denied" error. However, because the script determines whether the Web page is available, you may want the user name/password prompt to appear (to avoid exposing the admin password). Therefore, if a user name/password is specified (i.e., the user name and password are *not* blank), set this parameter to n. If no user name/password is specified (i.e., if the user name or password is blank), set this parameter to y. The default is y.
Number of times to retry after a fail	Specify the number of times to retry the connection. The default is 3 times.
Amount of time to wait between retries	Specify the number of seconds to wait for a connection before timing out and returning an error. The default is 0 seconds.
Event severity when Web page is inaccessible	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.
Monitor IIS server and site(s)?	Set to **y** to monitor the IIS server and associated sites. The default is y.
Auto-start monitored server and site(s)?	Set to **y** to automatically restart down IIS servers and sites. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager has been set not to restart the service. The default is 18.

CCMAdmin User Name and Password Configuration

If you require a user name and password for access to your `ccmadmin` Web page, configure that information into AppManager Security Manager. Then, when you run CCM_SecureWebPageCheck or CCM_WebPageCheck, the script will have authority to access the Web page.

On the Custom tab in AppManager Security Manager, complete the following fields:

Field	Description
Label	CCMADMIN
Sub-label	User name required for accessing the ccmadmin Web page
Value 1	Password required for accessing the ccmadmin Web page
Extended application support	Encrypts the user name and password in Security Manager. Do not leave this option unselected.

CCM_SystemPerformance

Use this Knowledge Script to monitor Cisco CallManager for call throttling, signals in queue, and severe and warning call-throttling states. Call throttling allows administrators to define CallManager performance parameters to limit the number of incoming calls from phones, IOS gateways, MGCP gateways, and MGCP PRI gateways. The CallManager code red and code yellow call-throttling states map to AppManager severe and warning level states, respectively.

Note
This script is supported only for CallManager versions 3.3(4) and later.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Monitor Call Throttling	
Event Notification	
Raised event if threshold is exceeded?	Select **Yes** to raise an event if either or both of the call throttling thresholds are exceeded. The default is Yes.
Threshold - Maximum rejected calls	Specify the maximum number of calls that can be rejected due to call throttling before an event is raised. The default is 10 calls.
Threshold - Maximum throttled skinny devices	Specify the maximum number of skinny devices that can be throttled before an event is raised. The default is 10 devices.
Event severity when rejected calls exceed the threshold	Set the severity level, from 1 to 40, to reflect the importance of an event in which the number of rejected calls exceeds the threshold that you set. The default is 5.
Event severity when throttled skinny devices exceed the threshold	Set the severity level, from 1 to 40, to reflect the importance of an event in which the number of throttled skinny devices exceeds the threshold that you set. The default is 5.
Raise event if severe call-throttling state entered?	Select **Yes** to raise an event if call throttling enters a severe (Code Red) state. The default is Yes.
Event severity when severe state entered	Set the severity level, from 1 to 40, to reflect the importance of an event in which call throttling has entered a severe state. The default is 5.
Raise event if warning call-throttling state entered?	Select **Yes** to raise an event if call throttling enters a warning (Code Yellow) state. The default is unselected.
Event severity when warning state entered	Set the severity level, from 1 to 40, to reflect the importance of an event in which call throttling has entered a warning state. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for call throttling?	Select **Yes** to collect data about calls rejected due to call throttling and about throttled skinny devices. The default is unselected.
Monitor Signals in Queue	
Event Notification	
Raise event if threshold is exceeded?	Select **Yes** to raise an event if either or both of the signal thresholds are exceeded. The default is Yes.
Threshold - Maximum high-priority signals in queue	Specify the maximum number of high-priority signals that can be in queue before an event is raised. The default is 500.
Threshold - Maximum normal-priority signals in queue	Specify the maximum number of normal-priority signals that can be in queue before an event is raised. The default is 1000.
Event severity when high-priority signals exceed the threshold	Set the severity level, from 1 to 40, to reflect the importance of an event in which the number of high-priority signals in queue exceeds the threshold that you set. The default is 5.
Event severity when normal-priority signals exceed the threshold	Set the severity level, from 1 to 40, to reflect the importance of an event in which the number of normal-priority signals in queue exceeds the threshold that you set. The default is 5.
Data Collection	
Collect data for signals in queue?	Select **Yes** to collect data about high and normal priority queue signals. The default is unselected.

CCM_SystemUsage

Use this Knowledge Script to monitor CPU and physical memory usage for the Cisco CallManager process, and total CPU and physical memory usage for the CallManager. If any threshold is exceeded, an event is raised. This script collects data about percentage of CPU and physical memory used by CallManager and percentage of CPU and physical memory used by the entire device. When monitoring a device without the CallManager process (such as a standalone Publisher) only the percentage of CPU and physical memory used by the device are collected. To make the most of the data collected by this script, run Report_SystemUsage.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Tip

On the Advanced tab, set the *Raise event if event condition occurs* parameter to **3** times within **3** job iterations to prevent the raising of events during peak usage.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about CPU and memory usage or reports and graphs. The default is y.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40,to indicate the importance of an event in which a threshold is exceeded. The default is 10.
Threshold - Maximum CallManager CPU usage	Specify the maximum percentage of CallManager CPU resources that can be used before an event is raised. The default is 65%.
Threshold - Maximum total CPU usage	Specify the maximum percentage of system CPU resources that can be used before an event is raised. The default is 80%.
Threshold - Maximum CallManager memory usage	Specify the maximum amount of CallManager memory resources that can be used before an event is raised. The default is 65%.
Threshold - Maximum total memory usage	Specify the maximum percentage of system memory resources that can be used before an event is raised. The default is 80%.

CCM_T1Channels

Use this Knowledge Script to monitor the number of active and in-service T1-CAS (channel associated signaling) channels for this CallManager. This script raises an event if a monitored value exceeds or falls below the threshold you set.

The ports or channels you monitor can be on one or more MGCP gateways.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if either threshold is breached. The default is y.
Collect data?	Set to **y** to collect data about T1-CAS channels for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls. The default is y.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Threshold - Maximum active T1-CAS channels	Specify the maximum number of T1-CAS channels that can be active before an event is raised. The default is 10 channels.
Threshold - Minimum T1-CAS spans in service	Specify the minimum number of T1-CAS spans that can be in service before an event is raised. The default is 0 channels.

CCM_WebPageCheck

Use this Knowledge Script to monitor accessibility to the `ccmadmin` and `ccmuser` Web pages and raise an event if the Web pages cannot be accessed. This script can collect data about the availability of the Web pages and round-trip connection time. If a URL is not reachable, the detail message records the reason (for example, because the format of the request was invalid or the server name was not found). If the Web pages cannot be accessed, you can arrange for this script to restart the IIS server and sites that are down.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Note
This script is not supported for Cisco CallManager versions 4.1 and later. If you are running 4.1 or later, use CCM_SecureWebPageCheck.

Resource Objects

CCM IIS Server

CCM IIS W3SRV

CCM IIS WebInst

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if Web page is inaccessible?	Set to **y** to raise an event if either Web page is inaccessible. The default is y.
Collect data for up/down URL?	Set to **y** to collect data about the up and down status of the URL. If set to y, the script returns a value of 100 if the connection is up and a value of 0 if the connection is down. The default is y.
Collect data for round-trip time?	Set to **y** to collect information about the round-trip connection time (in seconds). The default is n.
Monitor ccmadmin?	Set to **y** to monitor ccmadmin. The default is y.
Monitor ccmuser?	Set to **y** to monitor ccmuser. The default is y.
Username for ccmadmin	Enter the user name to use when logging on to ccmadmin. If a user name is not required, you can leave this field blank. For more information about the user name, see "CCMAdmin User Name and Password Configuration" on page 867. **Note** If you installed Cisco CallManager MLA (multi-level administration), this script will only verify that the ccmadmin Web page is present. It will not log in. Therefore, if you have MLA, there is no need to enter the user name.

Parameter	How to Set It
Treat Access Denied errors as "Up"?	When no password or user name is specified for ccmadmin, the URL check for ccmadmin will produce an "access denied" error. However, because the script determines whether the Web page is available, you may want the user name/password prompt to appear, to avoid exposing the admin password. Therefore, if the user name and password are not blank, set this parameter to n. If the user name or password is blank, set this parameter to y. The default is y.
Number of times to retry after a fail	Specify the number of times to retry the connection. The default is 3 times.
Amount of time to wait between retries	Specify the number of seconds to wait for a connection before timing out and returning an error. The default is 0 seconds.
Event severity when Web page is inaccessible	Set the event severity level, from 1 to 40,to indicate the importance of an event in which a Web page is inaccessible. The default is 8.
Monitor IIS server and site(s)?	Set to **y** to monitor the IIS server and associated sites. The default is y.
Auto-start monitored server and site(s)?	Set to **y** to automatically restart down IIS servers and sites. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager has not been set to restart the service. The default is 18.

CDRQuery

Use this Knowledge Script to query the CDR (Call Detail Records) table on the CallManager Publisher. The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the CDR tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in the CDR table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Diagnostic**. In diagnostic mode, this script runs once, and checks the CDR tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter. To run this script in diagnostic mode, select **Run once** on the Schedule tab.

Resource Object

CCM Publisher

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Options	
CDR database username	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Select event format	Select the format in which you want to receive the informational event: CSV, XML, or Both. The default is XML. • Select **CSV** (comma-separated value) to format an event message that can be forwarded to an Action script that is triggered by the event (if you have selected to initiate an Action script when an event is raised). • Select **XML** to format an event message that is not forwarded to an Action script. • Select **Both** to generate two event messages: one in CSV format, which is forwarded to an Action script, and one in XML format. If you select **Both**, the CSV event is collapsed under the XML event; it is not displayed in the Operator Console. To access the CSV event, turn off "Collapse duplicate events into a single event" on the Advanced tab before running this script. **Note** Error messages are formatted in plain text — this parameter does not apply to error messages.

Parameter	How to Set It
Columns to return	Select the columns that you want returned from the query: All, Basic, or Minimal. The default is Basic. Choose **All** to return all columns in the CDR table. Different versions of CallManager contain different columns in the CDR tables; you should check your CallManager documentation to see which columns you have. Choose **Basic** to return the following columns: • origDeviceName • origIpAddr • callingPartyNumber • origMediaCap_payloadCapability • destDeviceName • destIpAddr • originalCalledPartyNumber • finalCalledPartyNumber • destMediaCap_payloadCapability • dateTimeOrigination • dateTimeConnect • dateTimeDisconnect • duration • originalCalledPartyNumberPartition • callingPartyNumberPartition • finalCalledPartyNumberPartition • origCause_value • destCause_value Choose **Minimal** to return the following columns: • origDeviceName • origIpAddr • callingPartyNumber • destDeviceName • destIpAddr • originalCalledPartyNumber • finalCalledPartyNumber • dataTimeConnect • dataTimeDisconnect • duration
Collect data?	Set to **y** to collect data for graphs and charts. This script collects one data stream for the number of records found. The default is n.
Threshold	
Threshold - Maximum matching records	Specify how many records must match the specified query before an event is raised. The default is 0, which means that an event is raised if at least one record matches the query.
Query Filters	
Minimum duration	Set this parameter to filter out records whose call duration is less than the specified value. Accept the default of **0** if you do not want to filter for minimum call duration.

Parameter	How to Set It
Maximum duration	Set this parameter to filter out records whose call duration is less than or equal to the specified value. Accept the default of **0** if you do not want to filter for maximum call duration.
Calling directory number	Set this parameter to the number of the calling directory that you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any calling directory number.
Directory number connector	Set this parameter ONLY if you specify both a *Calling directory number* and a *Called directory number*. Your selection indicates how the script will connect the two parameters: AND or OR. The default is AND.
Called directory number	Set this parameter to the number of the called directory that you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any called directory number.
Originating device name	Set this parameter to query for those calls whose originating device name matches the specified value. Wildcard characters are acceptable. Leave this parameter blank to search for any originating device name.
Device name connector	Set this parameter ONLY if you specify both an *Originating device name* and a *Destination device name*. Your selection indicates how the script will connect the two parameters: AND or OR. The default is AND.
Destination device name	Set this parameter to query for those calls whose destination device name matches the specified value. Wildcard characters are acceptable. Leave this parameter blank to search for any destination device name.
Events	
Raise event if threshold is exceeded?	Set to **y** to raise an event if the matching records threshold is exceeded. The default is y.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.
Event severity when no records are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the script finds no records in the CDR. Accept the default of **0** if you do not want to raise an event for this situation.
Custom event message	Provide a custom message for the event, such as "Calls to 911" or "Calls exceeding 30 minutes." The default message is "# of records exceeded the threshold."
Diagnostics	
Select call disconnect time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **Note** This parameter is valid only when you select **Run once** on the Schedule tab.

CiscoBackupStatus

Use this Knowledge Script to monitor the Cisco IP Telephony Applications Backup Utility (`stiBack.exe`) program or the Cisco BARS (Backup and Restore System) program. This script verifies that the corresponding backup service is running and restarts the service if you choose. It reads the backup log to check the status of the previous backup. This script raises an event if the previous backup failed and can raise an event for successful backups.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Object

CCM Backup Utility

Default Schedule

By default, this script runs every two hours.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Auto-start backup service?	Select **Yes** to automatically restart stiBack.exe or BARS if it is down. The default is Yes.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the service is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the service was down but AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "No"	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the service is down and that AppManager has been set to not restart it. The default is 18.
Event Notification	
Raise event if backup succeeds?	This script always raises an event when it determines that the backup has failed. In addition, you can set this parameter to **Yes** to raise an event when the script determines that the backup has succeeded. The default is Yes.
Event severity when backup succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which backup succeeds. The default is 25.
Event severity when backup fails	Set the event severity level, from 1 to 40, to reflect the importance an event in which backup fails. The default is 5.
Ignore DC Directory service errors?	Select **Yes** to ignore errors related to the DC Directory service, such as failures to restore, stop, and restart. The default is unselected.

ConfBridgeActiveConf

Use this Knowledge Script to monitor the number of active conferences for a Conference Bridge. If the number of active conferences exceeds the threshold, an event is raised.

Resource Object

CCM Conference Bridge object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about active conferences for graphs and reports. The default is n.
Threshold - Maximum active conferences	Specify the maximum number of conferences that can be active before an event is raised. The default is 20.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

ConfBridgeActiveStreams

Use this Knowledge Script to monitor the number of active streams for a Conference Bridge. This script raises an event if the number of active streams exceeds the threshold.

Resource Object

CCM Conference Bridge object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about active streams for graphs and reports. The default is n.
Threshold - Maximum active streams	Specify the maximum number of streams that can be active before an event is raised. The default is 20.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

ConfBridgeAvailStreams

Use this Knowledge Script to monitor the number of available streams for a Conference Bridge. This script raises an event if the number of available streams falls below the threshold.

Resource Object

CCM Conference Bridge object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is not met?	Set to **y** to raise an event if the number of available streams falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about available streams for graphs and reports. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to “backup." By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls. The default is y.
Threshold - Minimum available streams	Specify the minimum number of streams that can be available before an event is raised. The default is 20.
Event severity when threshold is not met	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is not met. The default is 25.

ConfBridgeConferences

Use this Knowledge Script to monitor the number of conferences completed during an interval. This script raises an event if the number of completed conferences exceeds the threshold.

Resource Object

CCM Conference Bridge object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about completed conferences for graphs and reports. The default is n.
Threshold - Maximum completed conferences	Specify the maximum number of conferences that can be completed before an event is raised. The default is 20.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

ConfBridgeStreams

Use this Knowledge Script to monitor the number of streams on conferences that were completed during an interval. This script raises an event if the number of streams exceeds the threshold.

Resource Object

CCM Conference Bridge object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about conference bridge streams for graphs and reports. The default is n.
Threshold - Maximum streams	Set the threshold for the number of streams. If the number exceeds this amount, an event is raised. The default is 20.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

CTI_Manager

Use this Knowledge Script to monitor the number of CTI (Computer Telephony Interface) manager connections, open devices, open lines, and active CallManager links. This script raises an event if a value exceeds or falls below a threshold you set.

Resource Object

CCM CTI object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is breached. The default is y.
Collect data?	Set to **y** to collect data about connections, devices, lines, and links for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls. The default is y.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Threshold - Maximum active CallManager links	Specify the maximum number of CallManager links that can be active before an event is raised. Enter -1 to ignore this parameter. The default is 10.
Threshold - Minimum active CallManager links	Specify the minimum number of CallManager links that can be active before an event is raised. Enter -1 to ignore this parameter. The default is 0.
Threshold - Maximum CTI connections	Specify the maximum number of CTI connections that can occur before an event is raised. Enter -1 to ignore this parameter. The default is 100.
Threshold - Minimum CTI connections	Specify the minimum number of CTI connections that can occur before an event is raised. Accept the default of -1 to ignore this parameter.
Threshold - Maximum open CTI devices	Specify the maximum number of CTI devices that can be open before an event is raised. Enter -1 to ignore this parameter. The default is 100.
Threshold - Minimum open CTI devices	Specify the minimum number of CTI devices that can be open before an event is raised. Accept the default of -1 to ignore this parameter.
Threshold - Maximum open CTI lines	Specify the maximum number of CTI lines that can be open before an event is raised. Enter -1 to ignore this parameter. The default is 100.
Threshold - Minimum open CTI lines	Specify the minimum number of CTI lines that can be open before an event is raised. Accept the default of -1 to ignore this parameter.

DigitalOutboundBusy

Use this Knowledge Script to monitor the number of times during an interval that a call through this digital access was attempted when no ports were available. This script raises an event if the number of outbound busy attempts exceeds the threshold.

Resource Object

CCM Digital Access object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about outbound busy attempts for graphs and reports. The default is n.
Threshold - Maximum outbound busy attempts	Specify the maximum number of outbound busy attempts that can occur before an event is raised. The default is 100.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the template is exceeded. The default is 25.

DigitalPortsActive

Use this Knowledge Script to monitor the number of active digital ports. This script raises an event if the number of active digital ports exceeds the threshold.

Resource Object

CCM Digital Access object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about active ports for graphs and reports. The default is n.
Threshold - Maximum active ports	Specify the maximum number of ports that can be active before an event is raised. The default is 20.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

DigitalPortsOutOfService

Use this Knowledge Script to monitor the number of digital ports that are out of service. This script raises an event if the number of out-of-service digital ports exceeds the threshold.

Resource Object

CCM Digital Access object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about out-of-service ports for graphs and reports. The default is n.
Threshold - Maximum active ports	Specify the maximum number of ports that can be active before an event is raised. The default is 2.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active ports exceeds the threshold. The default is 15.

H323CallActivity

Use this Knowledge Script to monitor completed calls, attempted calls, and incomplete calls on H.323 devices for CallManager 4.2. This script raises an event if a threshold is exceeded. In addition, this script can generate the following data streams:

- Completed calls per device
- Completed calls for all devices
- Attempted calls per device
- Attempted calls for all devices
- Incomplete calls (%) per device
- Incomplete calls (%) for all devices

Tip
Use the Objects tab to limit the devices you want to monitor. Then use the parameters on the Values tab to monitor the devices individually or as a group.

Resource Object

CCM H.323 Device object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the H323CallActivity job fails. The default is 5.
Monitor Devices Individually	
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if attempted calls exceed threshold?	Select **Yes** to raise an event if the number of attempted calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum attempted calls	Specify the maximum number of calls that can be attempted before an event is raised. The default is 0 attempts.

Parameter	How to Set It
Event severity when attempted calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of attempted calls exceeds the threshold. The default is 15.
Raise event if percentage of incomplete calls exceeds threshold?	Select **Yes** to raise an event if the percentage of incomplete calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of incomplete calls	Specify the maximum percentage of incomplete calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of incomplete calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of incomplete calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per monitored device. The default is unselected.
Collect data for attempted calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of attempted calls per monitored device. The default is unselected.
Collect data for percentage of incomplete calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of incomplete calls per monitored device. The default is unselected.
Monitor Devices as a Group	
Name for this group of devices	Specify a name by which to identify the devices you selected on the **Objects** tab. Leave this field blank to accept the default group name: `H323_Group_JobID`.
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if attempted calls exceed threshold?	Select **Yes** to raise an event if the number of attempted calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum attempted calls	Specify the maximum number of calls that can be attempted before an event is raised. The default is 0 attempts.
Event severity when attempted calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of attempted calls exceeds the threshold. The default is 15.
Raise event if percentage of incomplete calls exceeds threshold?	Select **Yes** to raise an event if the percentage of incomplete calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of incomplete calls	Specify the maximum percentage of incomplete calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of incomplete calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of incomplete calls exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per group. The default is unselected.
Collect data for attempted calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of attempted calls per group. The default is unselected.
Collect data for percentage of incomplete calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of incomplete calls per group. The default is unselected.

H323CallsAttempted

Use this Knowledge Script to monitor the number of calls attempted by an H.323 device during an interval. This script raises an event if a threshold is exceeded.

Resource Object

CCM H.323 Device object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about attempted H.323 calls for graphs and reports. The default is n.
Threshold - Maximum attempted calls	Specify the maximum number of H.323 calls that can be attempted before an event is raised. The default is 100.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

H323CallsInProgress

Use this Knowledge Script to monitor the number of calls in progress for an H.323 device. This script raises an event if a threshold is exceeded.

Resource Object

CCM H.323 Device object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about in-progress H.323 calls for graphs and reports. The default is n.
Threshold - Maximum in-progress calls	Specify the maximum number of calls that can be in progress before an event is raised. The default is 20.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

IIS_CpuHigh

Use this Knowledge Script to monitor CPU usage for IIS application processes. This script raises an event if CPU usage exceeds the threshold that you set.

Resource Object

CCM IIS Server

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if CPU usage exceeds the threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data for CPU usage?	Set to **y** to collect data about CPU usage for reports and graphs. The default is n.
Process names	Specify the name of the application processes you want to monitor. The default is `inetinfo`. Separate multiple entries with commas. For example: `inetinfo,dllhost` **Note** Do not append .exe to the process names.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU resources the selected process can use before an event is raised. The default is 60%.
Event severity when CPU usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 8.

IIS_HealthCheck

Use this Knowledge Script to check IIS servers, Web site status, and the queue length for blocked I/O requests. If any server or Web site is not running, an event is raised. In addition, you can choose to automatically restart the IIS server or Web site. If the blocked I/O queue length is longer than the specified threshold, an event is raised.

This script monitors only Web sites (servers), not FTP sites, NNTP sites, or SMTP sites.

Resource Objects

CCM IIS server

CCM IIS FTP server

CCM IIS W3SRV

CCM IIS WebInst

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Auto-start monitored server(s)?	Set to **y** to automatically restart down servers. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager has been set not to restart the service. The default is 18.
Event severity for blocked I/O requests	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of blocked requests exceeds the threshold. The default is 5.
Threshold - Maximum blocked I/O requests	Specify the maximum number of I/O requests that can be in queue before an event is raised. The default is 0 requests.
Monitor IIS server?	Set to **y** to monitor the IIS server. The default is y.
Monitor FTP server?	Set to **y** to monitor the FTP server. The default is n.

IIS_KillTopCPUProcs

Use this Knowledge Script to monitor the CPU usage for the IIS `dllhost` and `mtx` processes. If one or both processes exceed the CPU usage threshold you set, an event is raised. You can set this script to automatically stop a process that exceeds the CPU usage threshold.

Resource Object

CCM IIS server

Default Schedule

By default, this script runs every three minutes.

Setting Parameters Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if kill is successful or unsuccessful?	Set to **y** to raise an event if an attempt to stop a process is successful or unsuccessful. The default is y.
Kill CPU-intensive processes?	Set to **y** to automatically stop any process that exceeds the threshold. The default is n.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU usage allowed by the dllhost and mtx processes before an event is raised. The default is 90%.
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 10.
Event severity when kill fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a process is exceeding the threshold and AppManager cannot stop the process. The default is 10.
Event severity when kill succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a process is exceeding the threshold and AppManager has successfully stopped the process. The default is 20.

IIS_MemoryHigh

Use this Knowledge Script to detect whether an IIS application process has exceeded the memory usage threshold you set. This script monitors the number of bytes of memory being used by the specified process. This script raises an event if an application process exceeds the memory usage threshold you set.

Resource Object

CCM IIS server

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about memory usage for reports and graphs. The default is n.
Process names	Specify the name of the application process you want to monitor. The default is `inetinfo`. Use a comma to separate multiple entries — do not use spaces. For example: `inetinfo,dllhost` **Note** Do not append .exe to the process names.
Threshold - Maximum memory usage	Specify the maximum amount of memory the selected process can use before an event is raised. The default is 10000000 bytes.
Threshold - Maximum memory pool usage	Specify the maximum amount of memory pool the selected process can use before an event is raised. The default is 5000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.

IIS_RestartServer

Use this Knowledge Script to restart an IIS server. This script raises an event if the server either successfully restarts or fails to restart.

Resource Object

CCM IIS server

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Wait N seconds before restarting	Specify the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is five seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the server. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart the server. The default if 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the server. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the server. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the server. The default is 25.

IIS_ServiceUpTime

Use this Knowledge Script to monitor the uptime for Web sites and services. This script raises an event if the amount of time the sites and services are running is less than the threshold you set.

Note
This script supports IIS versions 5 and later.

Resource Objects

IIS Web server and FTP server

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if uptime falls below threshold?	Set to **y** to raise an event in uptime falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about service uptime for reports and graphs. The default is n.
Threshold - Minimum uptime	Specify the minimum amount of uptime that is required for Web/FTP sites and services to prevent an event from being raised. The default is 10000 seconds.
Event severity when uptime falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which uptime falls below the threshold. The default is 5.

LineStatus

Use this Knowledge Script to monitor the status (number of active calls) of an individual phone line. This script raises an event if the number of calls exceeds the threshold.

Resource Objects

CCM Lines folder

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about line status for graphs and reports. The default is n.
Phone lines	Enter a comma-separated list of phone names to which you want to test communication.
Threshold - Maximum calls	Specify the most calls a phone line can have before an event is raised. The default is 1 call.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

LocationBandwidth

Use this Knowledge Script to monitor bandwidth statistics for a Location resource, if that resource has been defined in CallManager.

The Locations feature in Cisco CallManager provides call admission control for centralized call processing systems. Call admission control enables you to control the audio quality of calls over a wide area (IP WAN) link by limiting the number of calls allowed on the link at the same time. A centralized system uses a single Cisco CallManager cluster to control all of the locations.

In a centralized call processing system, the Cisco CallManager cluster resides at the main location along with other devices such as phones and gateways. Remote locations, such as branch offices of your company, house additional phones and other devices, but do not contain any call processing capability. The remote locations connect to the main location and to each other by means of IP WAN links.

Calls between devices at the same location do not need call admission control because those devices reside on the same LAN, which has unlimited available bandwidth. However, calls between devices at different locations must travel over an IP WAN link, which has limited available bandwidth. The Locations feature lets you specify the maximum amount of bandwidth available for calls to and from each location, thereby limiting the number of active calls and preventing oversubscription of the bandwidth on the IP WAN links.

For bandwidth calculations, CallManager assumes that each call consumes the following amount of bandwidth:

- G.711 calls use 80 kbps
- G.723 calls use 24 kbps
- G.729 calls use 24 kbps
- GSM calls use 29 kbps
- Wideband calls use 272 kbps

Resource Objects

CCM Location object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is breached. The default is y.
Collect data?	Set to **y** to collect data about bandwidth for reports and graphs. The default is n.

Parameter	How to Set It
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Threshold - Minimum available bandwidth	Specify the minimum amount of bandwidth that can be available before an event is raised. The default is 500 kbps.
Threshold - Maximum bandwidth in use	Specify the maximum amount of bandwidth that can be in use before an event is raised. The default is 75%.

LocationOutOfBandwidth

Use this Knowledge Script to monitor the number of times that calls through a particular Location failed due to lack of bandwidth. This script raises an event if the number of failures exceeds the threshold that you set. In addition, this script generates a data stream for the number of bandwidth failures.

Resource Object

CCM Location object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the LocationOutOfBandwidth job fails. The default is 5.
Monitor Out of Bandwidth Failures	
Event Notification	
Raise event if bandwidth failures exceed threshold?	Select **Yes** to raise an event if the number of calls that fail due to lack of bandwidth exceeds the threshold that you set. The default is 3 calls
Event severity when bandwidth failures exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of bandwidth failures exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for bandwidth failures?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that failed due to lack of bandwidth.

LossOfHardwarePhones

Use this Knowledge Script to monitor the number of registered hardware phones. This script raises an event if the number of lost phones exceeds a specified number or percentage during the monitored interval.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

You can also use this script to help you monitor phone status. For more information, see "CCM_PhoneInventory" on page 849.

Comparing Results of LossOfHardwarePhones and CCM_PhoneInventory

You can use the LossOfHardwarePhones script to launch an Action script that, in turn, launches the CCM_PhoneInventory script. By doing so, you can improve upon the results you get from LossOfHardwarePhones.

For example, say LossOfHardwarePhones indicates you have lost five phones since the last time it ran. But you configured the script to launch Action_RunPhoneInventory when the lost-phone event was raised, so CCM_PhoneInventory further refined the results. Based on criteria you selected, CCM_PhoneInventory identified the five phones by Directory Number, or Device Pool, or Subnet, or several other filtering options.

For several reasons, however, it is possible your results were inconsistent between LossOfHardwarePhones and CCM_PhoneInventory. Although you cannot fix the consistency problem, you can understand why it occurred:

- The scripts obtain phone data from two different sources. LossOfHardwarePhones uses the Performance Monitor counters on the Subscriber; CCM_PhoneInventory makes an API call to query phone information from the Publisher.
- The Subscriber and the Publisher can be out of sync because of the difference between timing windows or a lack of connectivity between the two devices. The information that is available from the two devices can change between the time LossOfHardwarePhones checks the counters and CCM_PhoneInventory makes its API call.
- Even if the Subscriber and the Publisher are in sync, differences in filtering can produce inconsistent results. The data from LossOfHardwarePhones is unfiltered — it includes everything; the data from CCM_PhoneInventory can be filtered by subnet, Directory Number, or several other filtering options.

Resource Object

CCM Subscriber

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Monitor Loss of Hardware Phones	
Event Notification	
Raise event if threshold is exceeded?	Select **Yes** to raise an event if a threshold is crossed. The default is Yes.
Threshold type	Select whether you want to set a threshold for the **Number** of lost phones or a **Percent** of hardware phones. The default is Percent.
Threshold - Maximum # lost hardware phones	Specify the maximum number of hardware phones that can be lost before an event is raised. The default is 24.
Threshold - Maximum % lost hardware phones	Specify the maximum percentage of hardware phones that can be lost before an event is raised. The default is 10%.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 10.
Data Collection	
Collect data for lost hardware phones?	Select **Yes** to collect data about lost phones for graphs and reports. The default is unselected.

MGCP_FXO

Use this Knowledge Script to monitor completed calls, outbound busy attempts, and blocked calls for Media Gateway Control Protocol (MGCP) Foreign Exchange Office (FXO) devices in CallManager 3.1 and 4.2.

This script raises an event if a threshold is exceeded. In addition, this script can generate the following data streams:

- Completed calls per device
- Completed calls for all devices
- Busy attempts per device
- Busy attempts for all devices
- Blocked calls (%) per device
- Blocked calls (%) for all devices

This script collects the data used by Report_MGCPDeviceUtil.

Tip
Use the Objects tab to limit the devices you want to monitor. Then use the parameters on the Values tab to monitor the devices individually or as a group.

Resource Object

CCM MGCP FXO object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MGCP_FXO job fails. The default is 5.
Additional event information	Provide any additional message text that you want to append to the Detailed Event Message of an event. You can enter up to 128 characters.
Monitor Devices Individually	
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.

Parameter	How to Set It
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per monitored device. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per monitored device. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per monitored device. The default is unselected.
Monitor Devices as a Group	
Name for this group of devices	Specify a name by which to identify the devices you selected on the Objects tab. Leave this field blank to accept the default group name: `FXO_Group_JobID`.
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.

Parameter	How to Set It
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per group. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per group. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per group. The default is unselected.

MGCP_FXS

Use this Knowledge Script to monitor completed calls, outbound busy attempts, and blocked calls for Media Gateway Control Protocol (MGCP) Foreign Exchange Station (FXS) devices in CallManager 3.1 and 4.2.

This script raises an event if a threshold is exceeded. In addition, this script can generate the following data streams:

- Completed calls per device
- Completed calls for all devices
- Busy attempts per device
- Busy attempts for all devices
- Blocked calls (%) per device
- Blocked calls (%) for all devices

This script collects the data used by Report_MGCPDeviceUtil.

Tip
Use the Objects tab to limit the devices you want to monitor. Then use the parameters on the Values tab to monitor the devices individually or as a group.

Resource Object

CCM MGCP FXS object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MGCP_FXS job fails. The default is 5.
Additional event information	Provide any additional message text that you want to append to the Detailed Event Message of an event. You can enter up to 128 characters.
Monitor Devices Individually	
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.

Parameter	How to Set It
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per monitored device. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per monitored device. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per monitored device. The default is unselected.
Monitor Devices as a Group	
Name for this group of devices	Specify a name by which to identify the devices you selected on the Objects tab. Leave this field blank to accept the default group name: `FXS_Group_JobID`.
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.

Parameter	How to Set It
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per group. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per group. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per group. The default is unselected.

MGCP_Gateway_CCM30

Use this Knowledge Script to monitor the station ports and voice channels for Media Gateway Control Protocol (MGCP) devices in CallManager 3.0. This script raises an event if a threshold is exceeded.

Resource Object

CCM MGCP Gateway object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about station ports and voice channels for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Monitor station ports?	Set to **y** to monitor station ports. The default is y.
Threshold - Maximum active station ports	Specify the maximum number of station ports that can be active before an event is raised. The default is 10 ports.
Monitor voice channels?	Set to **y** to monitor voice channels. The default is n.
Threshold - Maximum active voice channels	Specify the maximum number of voice channels that can be active before an event is raised. The default is 10 channels.

MGCP_Gateway_CCM31

Use this Knowledge Script to monitor the number of active MGCP Gateway station ports or voice channels for Media Gateway Control Protocol (MGCP) devices in CallManager 3.1 and later.

This script collects the data used by the Report_MGCPGatewayUsage Knowledge Script.

Resource Object

CCM MGCP Gateway object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is breached. The default is y.
Collect data?	Set to **y** to collect data about station ports and voice channels for reports and graphs. The default is n.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 15.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Monitor FXO ports?	Set to **y** to monitor FXO (foreign exchange office) ports. The default is n.
Threshold - Maximum active FXO ports	Specify the maximum number of FXO ports that can be active before an event is raised. The default is 10 ports.
Threshold - Minimum FXO ports in service	Specify the minimum number of FXO ports that must be in service to prevent an event from being raised. Accept the default of **0** to ignore this event.
Monitor FXS ports?	Set to **y** to monitor FXS (foreign exchange station) ports. The default is n.
Threshold - Maximum active FXS ports	Specify the maximum number of FXS ports that can be active before an event is raised. The default is 10 ports.
Threshold - Minimum FXS ports in service	Specify the minimum number of FXS ports that must be in service to prevent an event from being raised. Accept the default of **0** to ignore this event.
Monitor PRI voice channels?	Set to **y** to monitor PRI (primary rate interface) channels. The default is y.
Threshold - Maximum active PRI voice channels	Specify the maximum number of PRI voice channels that can be active before an event is raised. The default is 10 channels.

Parameter	How to Set It
Threshold - Minimum PRI channels in service	Specify the minimum number of PRI voice channels that must be in service to prevent an event from being raised. Accept the default of **0** to ignore this event.
Monitor T1_CAS voice channels?	Set to **y** to monitor T1-CAS (channel associated signaling) channels. The default is n.
Threshold - Maximum active T1-CAS voice channels	Specify the maximum number of T1 CAS voice channels that can be active before an event is raised The default is 10 channels.
Threshold - Minimum T1-CAS channels in service	Specify the minimum number of T1-CAS voice channels that must be in service to prevent an event from being raised. Accept the default of **0** to ignore this event.

MGCP_GatewayCheck

Use this Knowledge Script to monitor your CallManager for new and missing MGCP gateways. With each iteration of the job, this script creates a list of the MGCP gateways that are registered to the CallManager, and then compares the latest list information with the information from the previous list.

The list created by this script is sorted by the description of the MGCP gateway that you entered into CallManager.

Resource Object

CCM MGCP Gateway folder

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if new or missing gateways are found?	Set to **y** to raise an event if new MGCP gateways are found or if any gateway is missing within an interval that you specify. The default is y.
File name for saving list	Provide a name for the list of new or missing MGCP gateways. The default is `NQMGCPList`.
Raise event for the initial list?	Set to **y** to raise an event for the first time that this script creates a list. The default is n.
Event severity when MGCP gateways are missing	Set the severity level, from 1 to 40, to reflect the importance of an event in which MGCP gateways are missing. The default is 15.
Event severity when new MGCP gateways are found	Set the severity level, from 1 to 40, to reflect the importance of an event in which new MGCP gateways are found. Enter **0** if you do not want to raise an event. The default is 30.

MGCP_PRI

Use this Knowledge Script to monitor completed calls, outbound busy attempts, blocked calls, and data link availability for Media Gateway Control Protocol (MGCP) Primary Rate Interface (PRI) devices in CallManager 3.1 and 4.2.

This script raises an event if a threshold is exceeded. In addition, this script can generate the following data streams:

- Completed calls per device
- Completed calls for all devices
- Busy attempts per device
- Busy attempts for all devices
- Blocked calls (%) per device
- Blocked calls (%) for all devices

This script collects the data used by Report_MGCPDeviceUtil.

Tip
Use the Objects tab to limit the devices you want to monitor. Then use the parameters on the Values tab to monitor the devices individually or as a group.

Resource Object

CCM MGCP PRI object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MGCP_PRI job fails. The default is 5.
Additional event information	Provide any additional message text that you want to append to the Detailed Event Message of an event. You can enter up to 128 characters.
Monitor Devices Individually	
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.

Parameter	How to Set It
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Raise event if data link out of service?	Select **Yes** to raise an event if the PRI data link is out of service. The default is Yes.
Event severity when data link out of service	Set the severity level, from 1 to 40, to indicate the importance of an event in which the PRI data link is out of service. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per monitored device. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per monitored device. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per monitored device. The default is unselected.
Monitor Devices as a Group	
Name for this group of devices	Specify a name by which to identify the devices you selected on the Objects tab. Leave this field blank to accept the default group name: `PRI_Group_JobID`.
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.

Parameter	How to Set It
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per group. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per group. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per group. The default is unselected.

MGCP_PRI_Channels

Use this Knowledge Script to monitor an individual MGCP PRI device for active and out-of-service channels. In addition, you can run this script to monitor the number of active channels for a group of MGCP PRI devices. To monitor a group, run the script on the MGCP PRI Devices folder in the TreeView pane (instead of running it on an individual PRI device) and then use the Objects tab to select the PRI devices that you want to include in the group.

The first time you run this script, you can raise an informational event whose event message will contain the current status of all the channels being monitored. The possible statuses are listed below:

- 0 (unknown) - Indicates this channel is not defined. For example, channels 25-31 on T1-PRI devices are not defined. These channels are used by E1-PRI devices.
- 1 (out of service) - Indicates this channel is not available for use.
- 2 (idle) - Indicates this channel has no active call and is ready for use.
- 3 (busy) - Indicates an active call on this channel.
- 4 (reserved) - Indicates this channel has been reserved for use as a D-Channel or as a Synch-Channel for E1.

The detailed event messages and detailed data stream messages will contain the number of channels that are active or out-of-service.

The detailed event message and detailed data stream messages for a group of devices will contain the number of active channels for each device in the group.

This script collects the data used by the Report_MGCPChannelUsage Knowledge Script.

Note
If you use this script to monitor a group of devices, NetIQ Corporation recommends that you make a copy of the script and then rename it to something more specific to your needs, such as "Headquarter_Gateway_Activity" or "PSTN_Gateway_Actvity."

Resource Object

CCM MGCP PRI object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is y. This script can collect data streams for the number of active channels and, optionally, the number of out-of-service channels.

Parameter	How to Set It
Monitor these channels	Provide a range or a comma-separated list of the channel numbers that you want to monitor. You can enter a combination of range and list, such as 1-5,9,10,11,20-23. Separate each item by a comma. Valid channel numbers are 1-31. The default is 1-23.
Exclude these channels	Provide a range or a comma-separated list of the channel numbers that you want to exclude from monitoring. You can enter a combination of range and list, such as 1-5,9,10,11,20-23. Separate each item by a comma. Valid channel numbers are 1-31.
Threshold - Maximum active channels for any device	Specify the maximum number of monitored channels that can be active (status = 3) before an event is raised. The default is 20.
Event severity when active channels exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active channels exceeds the threshold. The default is 15.
Monitor out-of-service channels?	Set to **y** to monitor out-of-service channels. The default is y.
Threshold - Maximum out-of-service channels	Specify the maximum number of monitored channels that can be out-of-service (status = 1) for an individual device. If the number of out-of-service channels exceeds this amount, an event is raised. The default is 0 channels.
Event severity when out-of-service channels exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of out-of-service channels exceeds the threshold. The default is 5.
Collect data for out-of-service channels?	Set to **y** to collect data about the number of out-of-service channels for reports and graphs. The default is n.
Raise event with current status?	Set to **y** to create an event that indicates the current status of the channels. The default is n.
Additional event information	Enter any additional message text that you want to append to the Detailed Event Message for any events that are raised. You can enter up to 128 characters.
Monitor totals for a group of devices	Set to **y** to monitor all the devices in the group for which you are running this script. The default is y.
Name this group of PRI devices	If you are monitoring a group of PRI devices, enter a name for the group. This name will be displayed on events and charts. If no name is entered, this script generates a default name based on the current time.
Threshold - Maximum active channels for group of devices	Specify the maximum number of monitored channels that can be active (status = 3) for all devices in the group. If the number of active channels exceeds this amount, an event is raised. The default is 1250 channels.
Event severity when active channels for group exceed the threshold	Set the severity level, from 1 to 40, to indicate that the number of active channels for the entire group of PRI devices being monitored has exceeded the threshold. The default is 15.

MGCP_T1CAS

Use this Knowledge Script to monitor completed calls, outbound busy attempts, blocked calls, and data link availability for Media Gateway Control Protocol (MGCP) T1-CAS devices in CallManager 3.1 and 4.2.

This script raises an event if a threshold is exceeded. In addition, this script can generate the following data streams:

- Completed calls per device
- Completed calls for all devices
- Busy attempts per device
- Busy attempts for all devices
- Blocked calls (%) per device
- Blocked calls (%) for all devices

This script collects the data used by Report_MGCPDeviceUtil.

Tip
Use the Objects tab to limit the devices you want to monitor. Then use the parameters on the Values tab to monitor the devices individually or as a group.

Resource Object

CCM MGCP T1-CAS object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MGCP_T1CAS job fails. The default is 5.
Additional event information	Provide any additional message text that you want to append to the Detailed Event Message of an event. You can enter up to 128 characters.
Monitor Devices Individually	
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.

Parameter	How to Set It
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Raise event if data link out of service?	Select **Yes** to raise an event if the T1-CAS data link is out of service. The default is Yes.
Event severity when data link out of service	Set the severity level, from 1 to 40, to indicate the importance of an event in which the T1-CAS data link is out of service. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per monitored device. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per monitored device. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per monitored device. The default is unselected.
Monitor Devices as a Group	
Name for this group of devices	Specify a name by which to identify the devices you selected on the Objects tab. Leave this field blank to accept the default group name: `T1CAS_Group_JobID`.
Event Notification	
Raise event if completed calls exceed threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 200 calls.
Event severity when completed calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that can occur before an event is raised. The default is 0 attempts.

Parameter	How to Set It
Event severity when busy attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Raise event if percentage of blocked calls exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of blocked calls	Specify the maximum percentage of blocked calls that can occur before an event is raised. The default is 10%.
Event severity when percentage of blocked calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of blocked calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of completed calls per group. The default is unselected.
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts per group. The default is unselected.
Collect data for percentage of blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of blocked calls per group. The default is unselected.

MGCP_T1CAS_Channels

Use this Knowledge Script to monitor an individual MGCP T1-CAS device for active and out-of-service channels. In addition, you can run this script to monitor the number of active channels for a group of MGCP T1-CAS devices. To monitor a group, run the script on the MGCP T1-CAS Devices folder, instead of running it on an individual T1-CAS device. Then use the Objects tab to select the specific T1-CAS devices you want to include in the group.

The first time you run this script, you can choose to raise an informational event whose event message will contain the current status of all the channels being monitored. The possible statuses are listed below:

- 0 (unknown) - Indicates this channel is not defined.
- 1 (out of service) - Indicates this channel is not available for use.
- 2 (idle) - Indicates this channel has no active call and is ready for use.
- 3 (busy) - Indicates an active call on this channel.
- 4 (reserved) - Indicates this channel has been reserved for use as a D-Channel or as a Synch-Channel for E1.

This script collects the data used by the Report_MGCPChannelUsage Knowledge Script.

The detailed event messages and detailed data stream messages will contain the number of channels that are active or out-of-service.

The detailed event message and detailed data stream messages for a group of devices will contain the number of active channels for each device in the group.

Note
If you use this script to monitor a group of devices, NetIQ Corporation recommends making a copy of the script and renaming it to something more specific to your needs, such as "Headquarter_Gateway_Activity" or "PSTN_Gateway_Actvity."

Resource Object

CCM MGCP T1-CAS object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs.The default is y. This script can collect data streams for the number of active channels and, optionally, the number of out-of-service channels.

Parameter	How to Set It
Monitor these channels	Specify a range or a comma-separated list of the channel numbers that you want to monitor. You can enter a combination of range and list, such as 1-5,9,10,11,20-23. Separate each item by a comma. Valid channel numbers are 1-31. The default is 1-23.
Exclude these channels	Specify a range or a comma-separated list of the channel numbers that you want to exclude from monitoring. You can enter a combination of range and list, such as 1-5,9,10,11,20-23. Separate each item by a comma. Valid channel numbers are 1-31.
Threshold - Maximum active channels for any device	Specify the maximum number of monitored channels that can be active (status = 3) before an event is raised. The default is 20 channels.
Event severity when active channels exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 15.
Monitor out-of-service channels?	Set to **y** to monitor out-of-service channels. The default is y.
Threshold - Maximum out-of-service channels	Specify the maximum number of monitored channels that can be out-of-service (status = 1) for an individual device before an event is raised. The default is 0.
Event severity when out-of-service channels exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which out-of-service channels exceed the threshold. The default is 5.
Collect data for out-of-service channels?	Set to **y** to collect data about the number of out-of-service channels for reports and graphs. The default is n.
Raise event with current status?	Set to **y** to raise an event that indicates the current status of the channels. The default is n.
Additional event information	Provide any additional message text that you want to append to the Detailed Event Message of an event. You can enter up to 128 characters.
Monitor totals for a group of devices?	Set to **y** to monitor all the devices in the group for which you are running this script. The default is y.
Name this group of T1CAS devices	If you are monitoring a group of T1CAS devices, enter a name for the group. This name will be displayed on events and charts. If no name is entered, this script generates a default name based on the current time.
Threshold - Maximum active channels for all devices in group	Specify the maximum number of monitored channels that can be active (status = 3) for all devices in the group. If the number of active channels exceeds this amount, an event is raised. The default is 1250 channels.
Event severity when active channels for group exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the group's active channels exceed the threshold. The default is 15.

MLA_Logins

Use this Knowledge Script to scan CallManager MLA (multi-level administration) log files for successful and failed logins. In addition to information about successful and failed logins, the log files contain the user name, group name, date, and time of the login session.

Multi-level administration allows users with full access to configure different levels of administration access for CallManager administrators. Users with full access configure functional groups, user groups, and access privileges for user groups. In general, full-access users configure the access of other users to Cisco CallManager Administration.

The first time you run this script, you can check for the number of logins during the past n hours. Subsequent runs will check for the number of logins within the specified interval.

Resource Object

CCM MLA object

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about successful and failed logins for reports and graphs. The default is n.
Log file directory	Enter the directory path to the log file. The default is `c:\ciscoWebs\MLA\logs`
On first run, scan for logins in the past N hours	Enter the number of hours of log file entries through which the script will search for trace files. For instance, if you enter 15, the script will search through the last 15 hours of log file entries. The default is 1 hour. Setting this parameter to a high value may result in high CPU usage.
Threshold - Maximum failed logins	Specify the maximum number of logins that can fail before an event is raised. The default is 3 logins.
Threshold - Maximum successful logins	Set the threshold for the number of logons that have succeeded during the specified interval. If the number of successful logons exceeds this amount, an event is raised. The default is 3 logins.
Event severity when failed logins exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failed logins exceeds the threshold. The default is 5.
Event severity when successful logins exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of successful logins exceeds the threshold. The default is 25.

MOHDevice

Use this Knowledge Script to monitor the number of active and available resources for Music on Hold (MOH) devices.

MOH resources are provided by software-based MOH servers that register with CallManager. MOH servers are configured through CallManager Administration. Each MOH server is capable of supplying up to 500 Unicast output streams and 204 Multicast streams simultaneously, and can be configured for up to 51 different audio sources.

Resource Object

CCM MOH device object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a value exceeds or falls below a threshold. The default is y.
Collect data?	Set to **y** to collect data about MOH resources for reports and graphs. The default is n.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of an event in which a value exceeded or fell below a threshold. The default is 15.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Threshold - Maximum active Multicast connections	Specify the maximum number of Multicast connections that can be active before an event is raised. The default is 25 connections.
Threshold - Maximum active Unicast connections	Specify the maximum number of Unicast connections that can be active before an event is raised. The default is 250 connections.
Threshold - Minimum available Multicast connections	Specify the minimum number of Multicast connections that must be available to prevent an event from being raised. The default is five connections.
Threshold - Minimum available Unicast connections	Specify the minimum number of Unicast connections that must be available to prevent an event from being raised. The default is 50 connections.

MOHServer

Use this Knowledge Script to monitor active and available streams for Music on Hold (MOH) servers.

MOH resources are provided by software-based MOH servers that register with CallManager. MOH servers are configured through CallManager Administration. Each MOH server is capable of supplying up to 500 Unicast output streams and 204 Multicast streams simultaneously, and can be configured for up to 51 different audio sources.

Resource Object

CCM MOH server

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a value exceeds or falls below a threshold. The default is y.
Collect data?	Set to **y** to collect data about MOH devices for reports and graphs. The default is n.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of an event in which a value exceeded or fell below a threshold. The default is 15.
Threshold - Maximum active audio sources	Specify the maximum number of audio sources for the MOH server that can be active before an event is raised. The default is 25 sources.
Threshold - Maximum active Music On Hold streams	Specify the maximum number of MOH streams that can be active before an event is raised. The default is 200 streams.
Threshold - Minimum available Music On Hold streams	Specify the minimum number of MOH streams that must be available to prevent an event from being raised. The default is 50 streams.

MOHServer_LostConnections

Use this Knowledge Script to monitor the number of times that a Music on Hold (MOH) server lost connection with a CallManager.

MOH resources are provided by software-based MOH servers that register with CallManager. MOH servers are configured through CallManager Administration. Each MOH server is capable of supplying up to 500 Unicast output streams and 204 Multicast streams simultaneously, and can be configured for up to 51 different audio sources.

Resource Object

CCM MOH server

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if lost connections exceed the threshold?	Set to **y** to raise an event if the number of lost connections exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about lost connections for reports and graphs. The default is n.
Event severity when lost connections exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Threshold - Maximum lost connections	Specify the maximum number of lost connections that can occur before an event is raised. The default is 0 connections.

MTP_Device

Use this Knowledge Script to monitor the number of active and available resources for an individual MTP (media termination point) device. This script also monitors whether the MTP device ran out of resources at any time during the specified interval.

Resource Object

CCM MTP device object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a value exceeds or falls below a threshold. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is n. This script collects the number of active MTP resources.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a value exceeded or fell below a threshold. The default is 15.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a CallManager in backup mode.
Threshold - Maximum active resources	Specify the maximum number of MTP resources that can be active before an event is raised. The default is 20 resources.
Threshold - Minimum available resources	Specify the minimum number of MTP resources that must be available to prevent an event from being raised. The default is 0 resources.
Event severity when MTP device was out of resources	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MTP device ran out of resources at least once during the interval. Set to 0 to ignore an out-of-resource event. The default is 25. **Note** The event message for the out-of-resources event contains the number of times that the device ran out of resources.

MTPActiveConnections

Use this Knowledge Script to monitor the number of active connections for a Media Termination Point (MTP). An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

Resource Object

CCM Media Termination Point object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of active connections exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about active connections for reports and graphs. The default is n.
Threshold - Maximum active connections	Specify the maximum number of connections that can be active before an event is raised. The default is 20 connections.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active connections exceeds the threshold. The default is 25.

MTPActiveStreams

Use this Knowledge Script to monitor the number of active streams for a Media Termination Point (MTP). An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

Resource Object

CCM Media Termination Point object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about active streams for reports and graphs. The default is n.
Threshold - Maximum active streams	Specify the maximum number of streams that can be active before an event is raised. The default is 20 streams.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

MTPAvailableStreams

Use this Knowledge Script to monitor the number of available streams for a Media Termination Point (MTP). An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

Resource Object

CCM Media Termination Point object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is not met?	Set to **y** to raise an event if the number of available streams falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about available streams for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Threshold - Minimum available streams	Specify the minimum number of streams that must be available to prevent an event from being raised. The default is 20.
Event severity when threshold is not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of available streams falls below the threshold. The default is 25.

MTPCompletedConnections

Use this Knowledge Script to monitor the number of connections completed during an interval for a Media Termination Point (MTP). If the number of completed connections exceeds the threshold, an event is raised. An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

Resource Object

CCM Media Termination Point object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of completed connections exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about completed connections for reports and graphs. The default is n.
Threshold - Maximum completed connections	Specify the maximum number of connections that can be completed before an event is raised. The default is 20 connections.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of completed connections exceeds the threshold. The default is 25.

MTPCompletedStreams

Use this Knowledge Script to monitor the number of streams on connections completed during an interval for a Media Termination Point (MTP). An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

Resource Object

CCM Media Termination Point object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of completed streams exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about completed streams for reports and graphs. The default is n.
Threshold - Maximum completed streams	Specify the maximum number of streams that can be completed before an event is raised. The default is 20 streams.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of completed streams exceeds the threshold. The default is 25.

MTPsActive

Use this Knowledge Script to monitor the number of active Media Termination Points (MTP). An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of active MTPs exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about active MTPs for reports and graphs. The default is n.
Threshold - Maximum active Media Termination Points	Specify the maximum number of MTPS that can be active before an event is raised. The default is 50.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active MTPs exceeds the threshold. The default is 25.

MTPsAvailable

Use this Knowledge Script to monitor the number of Media Termination Points (MTP) available for use. An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is not met?	Set to **y** to raise an event if the number of available MTPs falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about available MTPs for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Threshold - Minimum available Media Termination Points	Specify the minimum number of MTPs that must be available to prevent an event from being raised. The default is 3.
Event severity when threshold is not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of available MTPs falls below the threshold. The default is 15.

MTPsUnavailable

Use this Knowledge Script to monitor the number of times during an interval that a Media Termination Point (MTP) allocation was requested when none was available. An MTP software device allows Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of out-of-resource instances exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about resource unavailability for reports and graphs. The default is n.
Threshold - Maximum out-of-resource instances	Specify the maximum number of times that MTP resources can be unavailable before an event is raised. The default is 0.
Event severity if threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of out-of-resource instances exceeds the threshold. The default is 5.

MulticastConfActive

Use this Knowledge Script to monitor the number of active Multicast conferences. This script raises an event if the number of active conferences exceeds the threshold.

Note
This script supports only Cisco CallManager version 3.0.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of active Multicast conferences exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about active conferences for reports and graphs. The default is n.
Threshold - Maximum active Multicast conferences	Specify the maximum number of Multicast conferences that can be active before an event is raised. The default is 50.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active Multicast conferences exceeds the threshold. The default is 25.

MulticastConfAvailable

Use this Knowledge Script to monitor the number of new Multicast conferences that can be started. This script raises an event if the number of available conferences is less than the threshold.

Note
This script supports only Cisco CallManager version 3.0.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is not met?	Set to **y** to raise an event if the number of available Multicast conferences falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about available conferences for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Threshold - Minimum available Multicast conferences	Specify the minimum number of Multicast conferences that must be available to prevent an event from being raised raised. The default is 3 conferences.
Event severity when threshold is not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of available Multicast conferences falls below the threshold. The default is 15.

MulticastConfCompleted

Use this Knowledge Script to monitor the number of Multicast conferences completed during an interval. This script raises an event if the number of completed conferences exceeds the threshold.

Note
This script supports only Cisco CallManager version 3.0.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of completed Multicast conferences exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about completed conferences for reports and graphs. The default is n.
Threshold - Maximum completed Multicast conferences	Specify the maximum number of Multicast conferences that can be completed before an event is raised. The default is 50 conferences.
Event severity if threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of completed Multicast conferences exceeds the threshold. The default is 25.

MulticastConfPhones

Use this Knowledge Script to monitor the number of active Multicast participants. This script raises an event if the number of participants exceeds the threshold.

Note
This script supports only Cisco CallManager version 3.0.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of active Multicast participants exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about Multicast participants for reports and graphs. The default is n.
Threshold - Maximum active Multicast participants	Specify the maximum number of Multicast participants that can be active before an event is raised. The default is 100 participants.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active Multicast participants exceeds the threshold. The default is 25.

MulticastConfUnavailable

Use this Knowledge Script to monitor the number of times during an interval that a Multicast conference was requested when none was available. This script raises an event if the threshold is exceeded.

Note
This script supports only Cisco CallManager version 3.0.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of out-of-resource instances exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about unavailable resources for reports and graphs.The default is n.
Threshold - Maximum out-of-resource instances	Specify the maximum number of out-of-resource instances that can occur before an event is raised. The default is 0 instances.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of out-of-resource instances exceeds the threshold. The default is 5.

QRTEvent

Use this Knowledge Script to monitor the log files of the Quality Reporting Tool (QRT). This script will start a diagnostic action and raise an event if a QRT request has been logged.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every minute.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Script Options	
QRT log file directory	Provide the file path to the QRT log file. The default is `C:\Program Files\Cisco\QRT`.
Maximum number of entries per event message	Specify the maximum number of entries that can be placed into a single event message. If more entries are found, a new event is raised. The default is five entries.
On first run, scan files modified in the last N minutes	Specify the number of minutes of previous activity through which the script will search the log file. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 30 minutes.
Monitor Quality Reporting Tool Log Entries	
Event Notification	
Raise event if new QRT log entry is found?	Select **Yes** to raise an event if a new QRT log entry is found. The default is Yes.
Event severity when new QRT log entry is found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a new log entry is found. The default is 5.
Data Collection	
Collect data for QRT log entries?	Select **Yes** to collect data about QRT log entries for reports and graphs. The default is unselected.

RegAnalogAccesses

Use this Knowledge Script to monitor the number of registered analog accesses. This script raises an event if the number of registered accesses exceeds the threshold.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of registered analog accesses exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about registered analog accesses for reports and graphs. The default is n.
Threshold - Maximum registered analog accesses	Specify the maximum number of analog accesses that can be registered before an event is raised. The default is 50 accesses.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of registered analog accesses exceeds the threshold. The default is 25.

RegCtiPorts

Use this Knowledge Script to monitor the number of CTI (Computer Telephony Interface) ports registered to the local CallManager.

A CTI port is a virtual device that can have one or more virtual lines. Software-based CallManager applications, such as SoftPhone, AutoAttendant, and IP Interactive Voice Response (IVR), can be configured to use CTI ports. You use the same CallManager Administration area to configure CTI ports that you use to configure phones. Because these virtual devices use up resources on the CallManager, you can use this script to monitor how many CTI ports are registered and to raise an event if this number exceeds a threshold you set.

This script queries the CallManager database for CTI ports.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if registered CTI ports exceed the threshold?	Set to **y** to raise an event if the number of registered CTI ports exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about registered CTI ports for reports and graphs. The default is n.
SQL username	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you have changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum registered CTI ports	Specify the maximum number of ports that can be registered before an event is raised. The default is 200 ports.
Event severity when registered CTI ports exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of registered CTI ports exceeds the threshold. The default is 25.

RegDigitalAccesses

Use this Knowledge Script to monitor the number of registered digital accesses. This script raises an event if the number of registered accesses exceeds the threshold.

Note
This script supports only Cisco CallManager version 3.0.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of registered digital accesses exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about registered digital accesses for reports and graphs. The default is n.
Threshold - Maximum registered digital accesses	Specify the maximum number of digital accesses that can be registered before an event is raised. The default is 50 accesses.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of registered digital accesses exceeds the threshold. The default is 25.

RegHardwarePhones

Use this Knowledge Script to monitor the number of registered hardware phones. This script raises an event if the number of registered hardware phones exceeds the threshold.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if registered hardware phones exceed the threshold?	Set to **y** to raise an event if the number of registered hardware phones exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about registered hardware phones for reports and graphs. The default is n.
Threshold - Maximum registered hardware phones	Specify the maximum number of hardware phones that can be registered before an event is raised. The default is 1000 phones.
Event severity when registered hardware phones exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of registered hardware phones exceeds the threshold. The default is 25.

RegMGCPGateways

Use this Knowledge Script to monitor the number of registered MGCP gateways. This script raises an event if the number of registered gateways falls below the threshold.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is not met?	Set to **y** to raise an event if the number of registered MGCP gateways falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about registered MGCP gateways for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Threshold - Minimum registered MGCP gateways	Specify the minimum number of MGCP gateways that must be registered to prevent an event from being raised. The default is 0 gateways.
Event severity when threshold is not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of registered MGCP gateways falls below the threshold. The default is 25.

RegOtherDevices

Use this Knowledge Script to monitor the number of registered station devices using the SCCP protocol (Skinny Protocol) that are not hardware phones, such as Cisco IP SoftPhones, Cisco uOne ports and Cisco Unity voice ports.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of registered “other” devices exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about registered “other” devices for reports and graphs.
Threshold - Maximum registered “other” devices	Specify the maximum number of “other” devices that can be registered before an event is raised. The default is 50 devices. I
Event severity if threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of registered “other” devices exceeds the threshold. The default is 25.

Report_CallActivity

Use this Knowledge Script to summarize the call activity for a selected time range for all CallManagers in a CallManager view. This report displays the data collected by the CallActivity script.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select the data for your report by view, computer, or data group. The default is View.
Select Knowledge Script	Select the scripts that collected the data you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Total by	Select the time period by which the data in your report is aggregated. The default is Hour.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
All data on a single chart?	Set to **y** to create a chart that displays all of the collected data. If you accept the default of **n**, the data is spread over several charts based on the following: • If you chose **Hour** in the "Total by" parameter, each chart will display a maximum of 48 data points. • If you chose **Day** in the "Total by" parameter, each chart will display a maximum of 14 data points.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.

Parameter	How to Set It
Select output folder	Set parameters for the output folder. The default folder name is CiscoCallMgrCallActivity.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager Call Activity.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Report_CallQualityDailyAvg

Use this Knowledge Script to display information about key call quality factors: jitter, latency, and lost data. This script uses the data collected by the CallQuality script.

CallQualityDailyAvg summarizes by hour, and weights by the total number of calls for each measured interval. For example, if you select two days of data, the chart represents the weighted average of all calls in a given hour for both days.

When running this script, take into consideration the following factors:

- The CallQuality script monitors only the jitter, latency, and lost data as seen from the originator of the call.
- The CallQuality script pulls its data from the actual Cisco CallManager database. It is possible that when the Monitoring script reads information from the database, CallManager may not have completed all updates to the database.
- There is no overall call-quality metric.

Note
If you want to report on call quality as seen by the recipient of the call, include real-time call quality data, or display an overall call quality metric, NetIQ Corporation recommends that you license the AppManager for VoIP Quality module, which provides more robust call-quality reporting.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select Knowledge Script(s)	Select the scripts that collected the data you want to use for the report. Select only those scripts that are applicable to this Report script.
Select CallManager Publisher	Select the CallManager Publisher on which you ran the Knowledge Script that you selected in the previous parameter.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Chart Thresholds	
Threshold - Jitter	Specify the jitter threshold to display on the jitter charts in the report. The default is 0 milliseconds.
Threshold - Latency	Specify the latency threshold to display on the latency charts in the report. The default is 0 milliseconds.
Threshold - Percent lost data	Specify the lost data threshold to display on the charts in the report. The default is 0%.

Parameter	How to Set It
Report Settings	
Include charts?	Set to **y** to include a chart in the report. The default is y.
Include table?	Set to **y** to include a table of information in the report. The default is y.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is CCMCallQualityDailyAvg.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager Call Quality Daily Average.
Select chart style	Select chart properties in the Chart Settings dialog box. The default style is Bar.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Report_CallsByHour

Use this Knowledge Script to summarize the active calls for all selected CallManagers in a selected time period.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select computer(s)	Select the computers that you want to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the scripts that collected the data you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include charts?	Set to **y** to include a chart in the report. The default is y.
Include tables?	Set to **y** to include a table of information in the report. The default is y.
Select chart properties	Select a chart type. The default style is Bar.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is CCMCallsByHour.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager Calls By Hour.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.

Parameter	How to Set It
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Report_ClusterAvgValueByHr

Use this Knowledge Script to display the average values by hour of the data streams for a CallManager cluster that were collected by a Knowledge Script within a specified time range.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select data wizard	Select the data for your report by view, computer, or data group.
Select the style	Select the style for the first page of the report: • By computer provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • By data stream provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers • By computer and data stream provides links to pages showing a single data stream collected from a computer • By Knowledge Script provides links to pages showing all data streams collected by a script (each page shows all data streams collected from all computers on which the script has run) • All data streams on one page generates a report with all data on a single page
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Aggregation interval	Select the time period by which the data in your report is aggregated. The default is 1 hour.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar_Stacked.

Parameter	How to Set It
Select output folder	Set parameters for the output folder. The default folder name is ClusterAvgValueByHr.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cluster Average By Hour.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Report_ClusterAvgValueByMin

Use this Knowledge Script to display the average values by minute of the data streams collected for a CallManager cluster by a Knowledge Script within a specified time range.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select the data for your report by view, computer, or data group.
Select the style	Select the style for the first page of the report: • By computer provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • By data stream provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers • By computer and data stream provides links to pages showing a single data stream collected from a computer • By Knowledge Script provides links to pages showing all data streams collected by a script (each page shows all data streams collected from all computers on which the script has run) • All data streams on one page generates a report with all data on a single page
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Aggregation interval	Select the time period by which the data in your report is aggregated. The default is 1 hour.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar_Stacked.

Parameter	How to Set It
Select output folder	Set parameters for the output folder. The default folder name is ClusterAvgValueByMin.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cluster Average By Minute.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Report_ClusterGenCounter

Use this Knowledge Script to display a chart showing the average, maximum, and minimum values of each CallManager cluster data stream and the actual data values of each data stream over time.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select the data for your report, either by view, computer, or data group.
Select the style	Select the style for the first page of the report: • By computer provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • By data stream provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers • By computer and data stream provides links to pages showing a single data stream collected from a computer • By Knowledge Script provides links to pages showing all data streams collected by a script (each page shows all data streams collected from all computers on which the script has run) • All data streams on one page generates a report with all data on a single page
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Maximum number of points per chart	Specify the maximum number of data points to include in the chart. The default is 200 points.
Select average, minimum, or maximum	Select the type of value you want to represent in your report. The default is AVG.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.

Parameter	How to Set It
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar_Stacked.
Select output folder	Set parameters for the output folder. The default folder name is ClusterGenCounter.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cluster General Counter.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Report_ClusterSystemUsage

Use this Knowledge Script to display the average CPU and memory usage per CallManager cluster within a specified time frame.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select cluster	Select a view and CallManager cluster for your report.
Select Knowledge Script(s)	Select the scripts that collected the data you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data.
Charts	
Include CPU usage chart?	Set to **y** to include a chart that details the CPU usage for the selected cluster. The default is y.
Include physical memory chart?	Set to **y** to include a chart that details the memory usage for the selected cluster. The default is y.
Chart threshold - CPU usage	Specify the CPU percentage threshold to display on the charts in the report. The default is 0%.
Chart threshold - Physical memory	Specify the physical memory threshold (in KB) to display on the charts in the report. The default is 0 KB.
Select chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Select chart color scheme	Select a color scheme template. The default is NetIQ1.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of information in the report. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is ClusterSystemUsage.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.

Parameter	How to Set It
Select properties	Set miscellaneous report properties as desired. The default report name is Cluster System Usage.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Report_MGCPChannelUsage

Use this Knowledge Script to display the average and maximum active channels for a particular MGCP PRI or T1-CAS Group within a specified time range. This report uses the data collected by the MGCP_PRI_Channels and MGCP_T1CAS_Channels scripts.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select device type	Select whether to report on PRI or T1-CAS devices.
Select Knowledge Script(s)	Select the scripts that collected the data you want to include in the report.
Select device groups	Select the MGCP PRI or T1-CAS Groups that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include charts?	Set to **y** to include a chart of data stream values in the report. The default is y.
Include tables?	Set to **y** to include a table of data stream values in the report. The default is y.
Select chart style for average values	Define the graphic properties of the charts in your report. The default style is Line.
Chart title	Provide a name for the chart in your report. The default title is Cisco CallManager MGCP Device Group Channel Usage.
All data on a single chart?	Set to **y** to display all data points on a single chart. The default is n. If you set to n, up to 24 data points are displayed on a single chart when aggregating by hour and up to 14 data points are displayed when aggregating by day.

Parameter	How to Set It
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is CiscoCallManager MGCPDeviceGroupChannelUsage.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager MGCP Device Group Channel Usage.
Add time stamp to title	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Report_MGCPDeviceUtil

Use this Knowledge Script to display average outbound busy attempts and calls completed for a particular MGCP PRI, T1-CAS, FXO, or FXS device within a specified time range. This report uses the data collected by the following scripts:

- MGCP_PRI
- MGCP_T1CAS
- MGCP_FXO
- MGCP_FXS

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select device type	Select whether to report on PRI, T1-CAS, FXO, or FXS devices.
Select Knowledge Script	Select the scripts that collected the data you want to include in the report.
Select device(s)	Select the PRI, T1-CAS, FXO, or FXS devices that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Chart Settings	
Chart threshold - Completed calls	Specify the completed calls threshold value to display on the charts in the report. The default is 0.
Chart threshold - Outbound busy attempts	Specify the outbound busy attempts threshold value to display on the charts in the report. The default is 0.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include charts?	Set to **y** to include a chart of data stream values in the report. The default is y.

Parameter	How to Set It
Include tables?	Set to **y** to include a table of data stream values in the report. The default is y.
Select chart style	Define the graphic properties of the charts in your report. The default style is Line.
Chart title	Provide a name for the chart in your report. The default title is Cisco CallManager MGCP Device Utilization.
All data on a single chart?	Set to **y** to display all data points on a single chart. The default is n. If you set to n, up to 24 data points are displayed on a single chart when aggregating by hour and up to 14 data points are displayed when aggregating by day.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is CiscoCallManager MGCPDeviceUtil.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager MGCP Device Utilization.
Add time stamp to title	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Report_MGCPGatewayUsage

Use this Knowledge Script to display the average number of active MGCP PRI and T1-CAS Voice Channels for a particular gateway within a specified time range. This report uses the data collected by the MGCP_Gateway_CCM31 script.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select Knowledge Script(s)	Select the scripts that collected the data you want to include in the report.
Select gateway(s)	Select the name of the MGCP gateways that you want to include in the report. You can include nor more than 10 gateways in a single report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is Sunday through Saturday.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include charts?	Set to **y** to include a chart of data stream values in the report. The default is y.
Include tables?	Set to **y** to include a table of data stream values in the report. The default is y.
Select chart style	Define the graphic properties of the charts in your report. The default style is Line.
Chart title	Provide a name for the chart in your report. The default title is Cisco CallManager MGCP Gateway Usage.
All data on a single chart?	Set to **y** to display all data points on a single chart. The default is n. If you set to n, up to 24 data points are displayed on a single chart when aggregating by hour and up to 14 data points are displayed when aggregating by day.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is CiscoCallManager MGCPGatewayUsage.

Parameter	How to Set It
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager MGCP Gateway Usage.
Add time stamp to title	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Report_ServicesAvailability

Use this Knowledge Script to summarize the availability (throughout the day) of the services most relevant to CallManager, for all CallManagers in a CallManager view. This report displays the data collected by the CCM_HealthCheck script.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select the data for your report, either by view, computer, or data group. The default is View.
Select Knowledge Script(s)	Select the scripts that collected the data you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CiscoCallMgrServicesAvailability.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager Services Availability.

Parameter	How to Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Report_SystemUsage

Use this Knowledge Script to display the processes that are using the most CPU and memory for a selected CallManager. The report can contain a table for top CPU usage, which will be displayed as a percentage averaged over the time interval, and another for top memory usage, which will be displayed in KB averaged over the time interval.

This script displays the data collected by the CCM_SystemUsage Knowledge Script.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the scripts that collected the data you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Charts	
Include CPU usage chart?	Set to **y** to include a chart that details the CPU usage for the selected cluster. The default is y.
Include memory usage chart?	Set to **y** to include a chart that details the memory usage for the selected cluster. The default is y.
Chart threshold - CPU usage	Specify the CPU percentage threshold to display on the charts in the report. The default is 0%.
Chart threshold - Memory usage	Specify the physical memory threshold (in KB) to display on the charts in the report. The default is 0 KB.
Select chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Select chart color scheme	Select a color scheme template. The default is NetIQ1.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.

Parameter	How to Set It
Include table?	Set to **y** to include a table of information in the report. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is CiscoCallMgrSystemUsage.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Cisco CallManager System Usage.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

SQL_Accessibility

Use this Knowledge Script to monitor SQL Server and database accessibility. This script raises an event if a SQL Server or a specified database is not accessible.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to **y** to collect data for reports and graphs. The default is n. If set to y, this script returns 100 if all specified databases are accessible, 50 if some of the specified databases are accessible and some are not, or 0 if none of the specified databases is accessible.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Database name	Provide a comma-separated list of the database names you want to monitor. For example, enter `master,pubs,tempdb`. If you leave this field blank, the script checks access to all databases. The default name is master.
Timeout	Specify a timeout period in seconds. The timeout period is the number of seconds to wait for a response before retrying or determining the database is inaccessible. The default is 0 seconds. **Note** This script continues waiting until it receives a response or the timeout is reached. During this waiting period, other jobs are blocked from execution. Therefore, limit your use of this parameter or keep the timeout period at a minimum for regular monitoring jobs. When you run this script to troubleshoot a particular problem and not a regularly scheduled interval for ongoing maintenance, you may want to adjust this parameter to allow a longer timeout period.
Number of retries	Specify the number of times to try connecting to the database before determining the database is inaccessible. The default is 0. **Note** This script continues waiting until it receives a response or has made the specified number of retry attempts. During this waiting period, other jobs are blocked from execution. Therefore, limit your use of this parameter or keep retry attempts at a minimum for regular monitoring jobs. When you run this script to troubleshoot a particular problem and not a regularly scheduled interval for ongoing maintenance, you may want to adjust this parameter to allow more retry attempts.

Parameter	How to Set It
Event severity when SQL Server or database is inaccessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which SQL Server or the database is inaccessible. The default is 5.

SQL_BlockedProcesses

Use this Knowledge Script to monitor the number of SQL processes that are blocked (queued) for longer than the period of time that you define. When the number of blocked processes is greater than the threshold, an event is raised.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every one minute.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if blocked processes exceed the threshold?	Set to **y** to raise an event if the number of blocked (queued) processes exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about blocked processes for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Blocked for duration	Specify the length of time that a process can be queued before it is considered a blocked process. The default is 500 milliseconds.
Threshold - Maximum blocked processes	Specify the maximum number of processes that can be blocked before an event is raised. The default is 5.
Number of blocked processes to display	Specify the number of processes to display in the Graph pane of the Operator Console. The default is 20.
Event severity when blocked processes exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

SQL_CPUUtil

Use this Knowledge Script to monitor the percentage of CPU resources used by the `sqlservr` and `sqlagent` processes. If the SQL Server processes exceed the threshold you set, an event is raised.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if CPU usage exceeds the threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about CPU usage for reports and graphs. The default is n.
Event severity when CPU usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 8.
Monitor the SQL Server process?	Set to **y** to monitor SQL Server. The default is y.
Threshold - Maximum CPU usage for SQL Server process	Specify the maximum amount of CPU resources that can be consumed by the SQL process before an event is raised. The default is 10%.
Monitor the SQL Agent process?	Set to y to monitor SQL Agent. The default is y.
Threshold - Maximum CPU usage for SQL Agent process	Specify the maximum amount of CPU resources that can be consumed by the SQL Agent process before an event is raised. The default is 10%.

SQL_DataGrowthRate

Use this Knowledge Script to monitor the data growth and shrink rates for all SQL Server databases. Growth and shrink rates are calculated by taking the difference of the data space utilization from the current interval from the data space utilization from the last interval. If these rates exceed the thresholds you set, an event is raised.

Resource Objects

CCM SQL Database folder

CCM SQL Database object

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval?	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y. Dynamic enumeration takes place only when the script runs on the Databases object, not when it runs on an individual database.
Exclude these objects	Provide a comma-separated list of the names of objects you want to exclude. For example, enter `master,model,mdb`. **Note** If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about growth and shrink rates for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**. **Note** If you are monitoring SQL Server 7, you need to use a sysadmin role account. Only members of the `sysadmin` role can get file statistics on SQL Server 7.0.
Threshold - Maximum growth rate	Specify the maximum percentage of data growth that is allowed between the last and current interval before an event is raised. The default is 25%.
Threshold - Maximum shrink rate	Specify the maximum percentage of data shrinkage that is allowed between the last and current interval before an event is raised. The default is 25%.

Parameter	How to Set It
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

SQL_DataSpace

Use this Knowledge Script to monitor the data space available and the percentage of data space being used for each database. This script raises an event if the available data space is lower or the percentage of data space used is higher than the threshold for any database.

You can set this script to discover new databases dynamically each time it runs. Discovering databases dynamically allows you to monitor data space for databases that have been added since running the SQL Discovery script and prevents you from attempting to monitor databases that have been dropped since discovery.

This script uses the `sysadmin` role account for SQL 7.0.

Resource Objects

CCM SQL Database folder

CCM SQL Database object

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval?	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y. Dynamic enumeration takes place only when the script runs on the Databases object, not when it runs on an individual database.
Exclude these objects	Provide a comma-separated list of the names of objects you want to exclude. For example: master,model,mdb **Note** If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is exceeded or not met. The default is y.
Collect data?	Set to y to collect data about available and used data space for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**. **Note** If you are monitoring SQL Server 7, you need to use a `sysadmin` role account. Only members of the sysadmin role can get file statistics on SQL Server 7.0.

Parameter	How to Set It
Threshold - Minimum available space	Specify the minimum amount of disk space that must be available to prevent an event from being raised. The default is 0 MB. Enter **0** to ignore this threshold.
Threshold - Maximum used space	Specify the maximum percentage of data space that can be used before an event is raised. The default is 90%.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded or not met. The default is 5.

SQL_DBGrowthRate

Use this Knowledge Script to monitor database growth and shrink rates. Growth and shrink rates are calculated by taking the difference between the database space utilization from the current interval and the database space utilization from the last interval. If these rates exceed the thresholds you set, an event is raised.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Objects

CCM SQL Database folder

CCM SQL Database object

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y. Dynamic enumeration takes place only when the script runs on the Database object, not when it runs on an individual database.
Exclude these objects	Provide a comma-separated list of the names of objects you do not want to monitor. For example: `master,model,mdb` **Note** If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about database growth and shrink rates for reports and graphs. The default is y.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**. **Note** If you are monitoring SQL Server 7, you need to use a sysadmin role account. Only members of the sysadmin role can get file statistics on SQL Server 7.0.
Update usage?	Set to **y** to have SQL Server recalculate the space usage. The default is n.
Threshold - Maximum growth rate	Specify the maximum percentage of database growth that is allowed between the last and current interval before an event is raised. The default is 25%.

Parameter	How to Set It
Threshold - Maximum shrink rate	Specify the maximum percentage of database shrinkage that is allowed between the last and current interval before an event is raised. The default is 25%.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

SQL_DbOption

Use this Knowledge Script to verify how SQL Server database options are set. You can select which options to check and whether to raise an event when an option is set (On) or not set (Off).

Resource Object

CCM SQL Database object

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when option is on?	Set to **y** to raise an event when the specified options are set. The default is y.
Raise event when option is off?	Set to **y** to raise an event when the specified options are not set. The default is n.
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, this script returns 100 if all of the specified options are on, 50 if some options are on, and 0 if no options are on. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Check all options?	Set to **y** to check all database options. The default is y.
Check ANSI null default option?	Set to **y** to check whether this option is on. When set, this database option controls whether database columns are null by default. The default is n.
Check ANSI nulls option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, all comparisons to a null value evaluate to unknown. The default is n.
Check ANSI warnings option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. This database option controls whether errors or warnings are issued when conditions such as "divide by zero" occur. The default is n.
Check auto_close option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, the database is shutdown cleanly and its resources are freed after the last user exits. The default is n.
Check auto_create statistics option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, statistics are automatically created on columns used in a predicate. The default is n.

Parameter	How to Set It
Check auto_update_statistics option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, existing statistics are automatically updated when the statistics become out-of-date. The default is n.
Check auto_shrink option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, the database files are candidates for automatic periodic shrinking. The default is n.
Check concat null yields null option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, if either operand in a concatenation operation is null, the result is null. The default is n.
Check cursor close on commit option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. When this database option is set to true, any cursors that are open when a transaction is committed or rolled back are closed. The default is n.
Check dbo use only option?	Set to **y** to check whether this option is on. This database option specifies that only the database owner can access the database. The default is n.
Check default to local cursor option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. This database option controls whether cursor declarations default to local. The default is n.
Check merge publish option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. This database option controls whether the database can be published for a merge replication. The default is n.
Check no chkpt on recovery option?	Set to **y** to check whether this option is on. When this database option is off, a checkpoint record is added to the database after a recovery/ restart operation. The default is n. This option is applicable only for SQL Server 6.x.
Check offline option?	Set to **y** to check whether the database is configured for offline operation. The default is n.
Check published option?	Set to **y** to check whether the database is configured for publishing (replication). The default is n.
Check quoted identifier option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. This database option controls whether double quotation mark characters can be used to surround delimited identifiers. The default is n.
Check read only option?	Set to **y** to check whether this option is on. When set, this database option specifies that database records are read-only; data cannot be modified. The default is n.
Check recursive triggers option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. This database option enables the recursive firing of raises. The default is n.
Check select into/bulkcopy option?	Set to **y** to check whether this option is on. When set, this database option allows unlogged database transactions. The default is n.
Check single user option?	Set to **y** to check whether this option is on. When set, this database option specifies that only one user can access the database at a time. The default is n.
Check subscribed option?	Set to **y** to check whether the database is configured as a subscriber database. The default is n.
Check torn page detection option?	Set to **y** to check whether this SQL Server 7.0 or 2000 option is on. This database option controls whether SQL Server detects incomplete pages. The default is n.

Parameter	How to Set It
Check trunc. log on chkpt option?	Set to **y** to check whether this option is on. This database option controls whether the transaction log is truncated when the Checkpoint process runs. The default is n.
Event severity when option is on or off	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored option is on or off. The default is 5.

SQL_DBSpace

Use this Knowledge Script to monitor available database space and the percentage of database space being used for each database. Database space includes both data space and log space. If the available database space exceeds the maximum threshold or falls below the minimum threshold you set, an event is raised.

You can set this script to discover new databases dynamically each time it runs. Discovering databases dynamically allows you to monitor database space for databases that have been added since running the Discovery_SQL Knowledge Script and prevents you from attempting to monitor databases that have been dropped since discovery.

Note
Although this script discovers databases each time it runs, the new databases are not reflected in the TreeView pane.

This script uses the `sysadmin` role account for SQL 7.0.

Resource Objects

CCM SQL Database folder

CCM SQL Database object

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y. Dynamic enumeration takes place only when the script runs on the Database object, not when it runs on an individual database.
Exclude these objects	Provide a comma-separated list of the names of objects you do not want to monitor. For example: `master,model,mdb` **Note** If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is exceeded or not met. The default is y.
Collect data?	Set to **y** to collect data about available and used database space for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.

Parameter	How to Set It
Update usage?	Set to **y** to have SQL Server recalculate the space usage. The default is n.
Threshold - Minimum available database space	Specify the minimum amount of disk space that must be available for the database (including data space and log space) to prevent an event from being raised. The default is 0 MB.
Threshold - Maximum used database space	Enter the maximum percentage of database space that can be used before an event is raised. The default is 90%.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded or not met. The default is 5.

SQL_Errorlog

Use this Knowledge Script to monitor the SQL Server error logs (`Errorlog`, `Errorlog.*` in `\MSSQL\LOG`). In the first interval, this script sets a starting point for future scanning. It does not scan the existing entries in the logs, and therefore it does not return any results on the first scan. As it continues to run at the interval specified in the Schedule tab, this script scans the logs for any new entries created since the last time it checked. This script raises an event if the number of entries that match the Find criteria exceeds the threshold you set.

Note
In general, the detail message for the script contains details about the occurrences found. If the message is larger than 32KB, the data is saved in a file on the managed computer (`<NetIQ_Home>\log`, for example, `C:\NetIQ\bin\log`) and the detail message contains the truncated data. If you generate these log files, you should periodically remove the files when you are done with them.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about log entries for reports and graphs. The default is n.
Case sensitive?	Set to **y** to match upper and lower case letters when checking for a match to the search string. The default is n.
Literal match?	Set to **y** if you only want to register a match when there is an exact match to the search string. If set to n, the log text containing any of the words in Find will be matched. For example, if you set this parameter to **y** and enter "foo bar" as the Find string, only lines containing "foo bar" are considered a match. If you set this parameter to n with the same string, any lines that contain "foo," "bar," or "foo bar" are considered a match. The default is n.
Find log text	Specify all or part of the text string you want to find. Separate multiple entries with a space. The default is deadlock.
Threshold - Maximum log text matches	Specify the maximum number of matching entries that can be found before an event is raised. If you accept the default of **0**, the first instance exceeds the threshold and raises an event.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 5.

SQL_LogGrowthRate

Use this Knowledge Script to monitor log growth and shrink rates for all SQL Server databases. Growth and shrink rates are calculated by taking the difference of the log space utilization from the current interval from the log space utilization from the last interval. This script raises an event if these rates exceed the thresholds you set.

Resource Objects

CCM SQL Database folder

CCM SQL Database object

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y. Dynamic enumeration takes place only when the script runs on the Database object, not when it runs on an individual database.
Exclude these objects	Provide a comma-separated list of the names of objects you do not want to monitor. For example: `master,model,mdb` **Note** If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is exceeded?	Set to **y** to raise an event if the growth or shrink rate exceeds its threshold. The default is y.
Collect data?	Set to **y** to collect data about growth and shrink rates for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**. **Note** If you are monitoring SQL Server 7, you need to use a sysadmin role account. Only members of the sysadmin role can get file statistics on SQL Server 7.0.
Threshold - Maximum growth rate	Specify the maximum percentage of log growth that is allowed between the last and current interval before an event is raised. The default is 25%.
Threshold - Maximum shrink rate	Specify the maximum percentage of log shrinkage that is allowed between the last and current interval before an event is raised. The default is 25%.

Parameter	How to Set It
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

SQL_LogSpace

Use this Knowledge Script to monitor a database's available log space and log space usage. If the available log space is lower or the percentage of log space used is higher than the threshold you set, an event is raised.

You can set this script to discover new databases dynamically each time it runs.

Note
Although this script discovers databases each time it runs, the new databases are not reflected in the TreeView pane.

This script uses the `sysadmin` role account for SQL 7.0.

Resource Objects

CCM SQL Database folder

CCM SQL Database object

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y.
Exclude these objects	Provide a comma-separated list of the names of objects you do not want to monitor. For example: `master,model,mdb` **Note** If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is exceeded or not met. The default is y.
Collect data?	Set to **y** to collect data about used and available log space for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Minimum available log space	Specify the minimum amount of log space that must be available to prevent an event from being raised. The default is 0 MB.
Threshold - Maximum used log space	Specify the maximum percentage of log space that can be used before an event is raised. The default is 90%.

Parameter	How to Set It
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded or not met. The default is 5.

SQL_MemUtil

Use this Knowledge Script to monitor the amount of memory that is used by SQL Server processes: `sqlservr` and `sqlagent`.

If using SQL Server 7.0 or 2000, you can use this script to monitor total server memory usage, number of free buffers, and memory usage.

If the amount of memory used by SQL Server exceeds the threshold you set, an event is raised.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about memory usage for reports and graphs. The default is n.
Threshold - Maximum process memory usage	Specify the maximum amount of memory that can be consumed by SQL Server before an event is raised. The default is 50000000 bytes.
Threshold - Maximum number of free buffers	Specify the maximum number of free buffers that can be in use before an event is raised. The default is 50 buffers.
Threshold - Maximum SQL Server memory usage	Specify the maximum amount of memory that can be in use by SQL Server and all related processes before an event is raised. The default is 30000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

SQL_NearFileMaxSize

Use this Knowledge Script to monitor the size of all SQL Server database files. This script enables you to set a threshold for when a file is reaching its maximum size. If any database file size exceeds the threshold you set, an event is raised.

You can set this script to discover new databases dynamically each time it runs.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Note
Although this script discovers databases each time it runs, the new databases are not reflected in the TreeView pane.

Resource Objects

CCM SQL DB File folder

CCM SQL DB File object

Default Schedule

By default, this script runs every 24 hours.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y.
Exclude these objects	Provide a comma-separated list of the names of objects you do not want to monitor. For example: `master,model,mdb` **Note** If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is exceeded?	Set to **y** to raise an event if a file's size exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about file size for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum file size	Specify the maximum size a database file can attain before an event is raised. The default is 500 MB.
Threshold - Maximum file size utilization	Specify the maximum percentage that a file can use of its maximum allowed size before an event is raised. The default is 90%.

Parameter	How to Set It
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

SQL_NearMaxConnect

Use this Knowledge Script to monitor the open connection usage of SQL Server. This script compares the current number of connections being used to the maximum number of connections configured for the server. This script raises an event if the used percentage (current connections/maximum connections) exceeds the threshold you set.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if used connections exceed the threshold?	Set to **y** to raise an event if the percentage of used connections exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about connection usage for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum used connections	Specify the maximum percentage of connections that can be in use before an event is raised. The default is 95%.
Event severity when used connections exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of used connections exceeds the threshold. The default is 5.

SQL_NearMaxLocks

Use this Knowledge Script to monitor the lock usage of SQL Server. This script compares the current number of locks being used to the maximum number of locks configured for the server. This script raises an event if the used percentage (current locks/maximum locks) exceeds the threshold you set.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if lock usage exceeds the threshold?	Set to **y** to raise an event if the percentage of used locks exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about lock usage for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum lock usage	Enter the maximum percentage of locks that can be in use before an event is raised. The default is 95%.
Event severity when lock usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which lock usage exceeds the threshold. The default is 5.

SQL_NetError

Use this Knowledge Script to monitor SQL Server network errors. This script compares the number of packet errors that occurred between the current and previous monitoring interval. This script raises an event if the number of errors exceeds the threshold you set.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if network errors exceed the threshold?	Set to **y** to raise an event if network errors exceed the threshold. The default is y.
Collect data?	Set to **y** to collect data about network errors for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum network errors	Specify the maximum number of network errors allowed before an event is raised. The default is 0 errors.
Event severity when network errors exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of network errors exceeds the threshold. The default is 5.

SQL_RepTransactions

Use this Knowledge Script to monitor the number of transactions in the transaction log of the publication database that are marked for replication but have not yet been replicated. This script raises an event if the number of transactions exceeds the threshold you set.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if pending transactions exceed the threshold?	Set to **y** to raise an event if the number of transactions awaiting replication exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about pending transactions for reports and graphs. The default is n.
Threshold - Maximum pending transactions	Specify the maximum number of transactions that can be awaiting replication before an event is raised. The default is 1000 transactions.
Event severity when pending transactions exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of transactions awaiting replication exceeds the threshold. The default is 5.

SQL_RepTranSec

Use this Knowledge Script to monitor the number of transactions being replicated per second. This script raises an event if the number of transactions exceeds the threshold you set.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if replicated transactions exceed the threshold?	Set to **y** to raise an event if the number of transactions replicated per second exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about replicated transactions for reports and graphs. The default is n.
Threshold - Maximum transactions replicated per second	Specify the maximum number of transactions that can be replicated per second before an event is raised. The default is 1000 transactions.
Event severity when replicated transactions exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of transactions replicated per second exceeds the threshold. The default is 5.

SQL_RestartServer

Use this Knowledge Script to restart SQL Server. This script raises an event if the server either successfully restarts or fails to restart.

To restart the SQL services, this script will also stop dependent CallManager services, such as Cisco Database Layer Monitor. These services will be automatically restarted.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Wait N seconds before restarting	Specify the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is five seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the server. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of event in which AppManager cannot restart the server. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the server. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the server. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the server. The default is 25.

SQL_ServerDown

Use this Knowledge Script to monitor the up/down status of SQL Server. If SQL Server is down, the script reports an event and, optionally, attempts to re-start SQL Server.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Auto-start SQL Server?	Set to **y** to automatically restart SQL Server if it is down. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot start SQL Server. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully starts SQL Server. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which SQL Server is down and auto-start is set to n. The default is 18.

SQL_ServerThroughput

Use this Knowledge Script to monitor SQL Server throughput by measuring the number of T-SQL batch requests executed per second and the number of physical page reads per second. This script raises an event if either threshold is exceeded.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about throughput for reports and graphs. The default is n.
Threshold - Maximum batch requests per second	Specify the maximum number of batch request transactions allowed per second before an event is raised. The default is 120 requests.
Threshold - Maximum page reads per second	Specify the maximum number of page reads allowed per second before an event is raised. The default is 100 page reads.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

SQL_TopIOUsers

Use this Knowledge Script to monitor the number of I/O read and write operations used by SQL Server users and their connections. This script raises an event if the number of operations exceeds the threshold. You can specify the number of top user connections to display in the detail event and data message.

The detail message includes user name, most recent SQL statements executed, spid, and the number of operations used by each user.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if I/O operations exceed the threshold?	Set to **y** to raise an event if the number if I/O read and writer operations exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about I/O operations for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Display T-SQL?	Set to **y** to display the executing T-SQL in the detail message. The default is y. **Note** The executing SQL statements are included in the detail message only when you use the sa login account.
Exclude these applications	Provide a comma-separated list of the names of applications you do not want to monitor. The default is SQLEXEC.
Number of top user connections to display	Specify the number of top user connections you want displayed in the detail message (event or data). Enter **0** if you want all user connections displayed. The default is 5 connections.
Threshold - Maximum I/O operations	Specify the maximum number of I/O operations allowed before an event is raised. The default is 9999999 operations. **Note** This number represents the cumulative operations for a user connection.
Event severity when I/O operations exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of I/O operations exceeds the threshold. The default is 5.

SQL_TopLockUsers

Use this Knowledge Script to monitor the total number of locks held by all SQL Server users and their connections. This script raises an event if the number of user locks held exceeds threshold you set.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if held user locks exceeds the threshold?	Set to **y** to raise an event if the number of held user locks exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about held locks for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Display T-SQL?	Set to **y** to display the executing T-SQL in the detail message. The default is y. **Note** The executing SQL statements are included in the detail message only when you use the sa login account.
Exclude these applications	Provide a comma-separated list of the names of applications you do not want to monitor. The default is SQLEXEC.
Threshold - Maximum held user locks	Specify the maximum number of user locks that can be held before an event is raised. The default is 1000 locks.
Number of top user connections to display	Specify the number of top user connections you want displayed in the detail message (event or data). Enter **0** if you want all user connections displayed. The default is five connections.
Event severity when held user locks exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of held user locks exceeds the threshold. The default is 5.

SQL_TopMemoryUsers

Use this Knowledge Script to monitor the memory that can be allocated to all SQL Server users and their connections in 2KB pages. This script raises an event if the total number of allocated pages exceeds the threshold you set.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if allocated memory pages exceed the threshold?	Set to **y** to raise an event if the number of allocated memory pages exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about allocated memory pages for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Display T-SQL?	Set to **y** to display the executing T-SQL in the detail message. The default is y. **Note** The executing SQL statements are included in the detail message only when you use the sa login account.
Exclude these applications	Provide a comma-separated list of the names of applications you do not want to monitor. The default is SQLEXEC.
Threshold - Maximum allocated memory pages	Specify the maximum number of 2-KB memory pages that can be allocated before an event is raised. The default is 15000 pages.
Number of top user connections to display	Specify the number of top user connections you want displayed in the detail message (event or data). Enter **0** if you want all user connections displayed. The default is five connections.
Event severity when allocated memory pages exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of allocated memory pages exceeds the threshold. The default is 5.

SQL_UserConnections

Use this Knowledge Script to monitor the total number of SQL Server user connections. This script raises an event if the total number of SQL Server user connections exceeds the threshold you set.

Resource Object

CCM SQL Server

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if user connections exceed the threshold?	Set to **y** to raise an event if the number of SQL Server user connections exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about SQL Server user connections for reports and graphs. The default is n.
SQL login	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Threshold - Maximum user connections	Specify the maximum number of user connections allowed before an event is raised. The default is 100 connections.
Number of user connections to display	Specify the number of user connections you want displayed in the detail message (event or data). Enter **0** to display all user connections. The default is 20 connections.
Event severity when user connections exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of user connections exceeds the threshold. The default is 5.

StreamApplOCTLErr

Use this Knowledge Script to monitor the number of times during an interval that an IOCTL (input/output control) error was detected. This script raises an event if the number of IOCTL errors exceeds the threshold.

Resource Object

CCM VoIP Application object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of detected errors exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about IOCTL errors for graphs and reports. The default is n.
Threshold - Maximum IOCTL errors	Specify the maximum number of IOCTL errors that can be detected before an event is raised. The default is 0.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of IOCTL errors exceeds the threshold. The default is 5.

StreamAppMissDDErr

Use this Knowledge Script to monitor the number of times during an interval that a missing device driver (DD) error was detected. This script raises an event if the number of missing driver errors exceeds the threshold.

Resource Object

CCM VoIP Application object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of errors exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about missing device driver errors for graphs and reports. The default is n.
Threshold - Maximum missing device driver errors	Specify the maximum number of missing device driver errors that can be detected before an event is raised. The default is 0.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of errors exceeds the threshold. The default is 5.

TftpChangeNotify

Use this Knowledge Script to monitor the number of TFTP change notifications handled during an interval. This script raises an event if the number of change notifications exceeds the threshold.

Resource Object

CCM TFTP object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of change notifications exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about TFTP change notifications for graphs and reports. The default is n.
Threshold - Maximum TFTP change notifications	Specify the maximum number of TFTP change notifications that can be handled before an event is raised. The default is 10.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of TFTP change notifications exceeds the threshold. The default is 25.

TftpErrors

Use this Knowledge Script to monitor the number of TFTP-related errors occurring during an interval. This script raise an event if a threshold is exceeded.

Resource Object

CCM TFTP object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if any threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about TFTP-related errors for graphs and reports. The default is n.
Threshold - Maximum aborted requests	Specify the maximum number of aborted requests that can occur before an event is raised. The default is 0 requests.
Threshold - Maximum NOT FOUND errors	Specify the maximum number of NOT FOUND errors that can occur before an event is raised. The default is 0. A NOT FOUND error is returned when a device requests a configuration file or firmware load, but the requested file does not exist in the TFTPPath of the TFTP server. Each time this error is returned, the TFTP server updates its NOT FOUND counter in perfmon. This script checks the NOT FOUND counter and raises an event if the number of NOT FOUND errors that occurred during the interval exceeds the threshold.
Threshold - Maximum overflow errors	Specify the maximum number of overflow errors that can occur before an event is raised. The default is 0. Overflow occurs when the TFTP service rejects some TFTP requests because it has reached the maximum number of allowable client connections. **Note** Overflow also occurs when the TFTP service is rebuilding configuration files; the TFTP service denies all requests while rebuilding files. If you don't want to generate an for requests that were denied during file rebuilding, you may want to click on the Advance tab and set this script to generate an event only if the overflow threshold is exceeded twice within two job iterations or three times within three job iterations. If events are generated more than three times in a row, you may have an overflow problem that requires your attention.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 25.

TftpHeartBeat

Use this Knowledge Script to monitor the Cisco TFTP heartbeat. This script raises an event if the heartbeat stops or is too low. In addition, this script generates a data stream for TFTP heartbeat data.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Object

CCM TFTP object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if heartbeat stops or falls below the threshold?	Set to **y** to raise an event if the heartbeat stops or falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about the TFTP heartbeat for graphs and reports. The default is n.
Threshold - Minimum heartbeat	Specify the minimum heartbeat count that must occur to prevent an event from being raised. The default is 500.
Event severity when heartbeat falls below the threshold	Set the event severity level, from 1 to 40,to indicate the importance of an event in which the heartbeat falls below the threshold. The default is 20.
Event severity when heartbeat stops	Set the event severity level, from 1 to 40,to indicate the importance of an event in which the heartbeat stops. The default is 10.

TftpRequests

Use this Knowledge Script to monitor the number of TFTP requests handled during an interval. This number includes local requests that were successfully handled by the server, "NotFound" requests, and requests that were aborted or rejected by the TFTP server.

This script is a member of a Recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Groups" on page 1030.

Resource Object

CCM TFTP object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of TFTP requests exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about TFTP requests for graphs and reports. The default is n.
Threshold - Maximum TFTP requests	Specify the maximum number of TFTP requests that can be handled before an event is raised. The default is 100 requests.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of TFTP requests exceeds the threshold. The default is 25.

TftpSegmentPctLost

Use this Knowledge Script to monitor the percentage of TFTP segments lost during an interval. This script raises an event if the percentage of lost segments exceeds the threshold.

Resource Object

CCM TFTP object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the percentage of lost TFTP segments exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about lost TFTP segments for graphs and reports. The default is n.
Threshold - Maximum lost segments	Specify the maximum percentage of lost segments that can occur before an event is raised. The default is 1%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of lost TFTP segments exceeds the threshold. The default is 15.

TftpSegmentsSent

Use this Knowledge Script to monitor the number of TFTP segments sent during an interval. This script raises an event if the number of sent segments exceeds the threshold.

Resource Object

CCM TFTP object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of sent segments exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about sent TFTP segments for graphs and reports. The default is n.
Threshold - Maximum sent TFTP segments	Specify the maximum number of TFTP segments that can be sent before an event is raised. The default is 100000 segments.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of sent TFTP segments exceeds the threshold. The default is 25.

TraceArchive

Use this Knowledge Script to archive CallManager trace files to avoid losing files when tracing wraps.

This script archives files based on the "last modified time" of each file, rather than the individual trace date or time stamp within each file.

Note
This script may be CPU-intensive based on the number of trace files the CallManager has collected. NetIQ Corporation recommends using this script for debugging purposes only — it may affect call processing.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Trace file directory	Provide the file path to the trace file. The default is `c:\program files\cisco\trace\ccm`.
Destination directory	Provide the file path of the archive file. The default is `c:\tracearchive`.
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search for trace files. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 30 minutes. **Note** Ensure that the time you set is smaller than the amount of time that it takes CallManager to wrap or begin overwriting files. CallManager's iteration time varies based on the trace output format, the debug tracing level, the maximum number of files, the maximum lines per file, and the maximum minutes per file specified within the CallManager Serviceability tool. The larger the call volume, the faster CallManager will fill the trace files.

TraceEvent

Use this Knowledge Script to scan CallManager trace files for entries that match a text string that you specify. This script raises an event when matching entries are found.

Note
This script may be CPU-intensive based on the number of trace files the CallManager has collected. NetIQ Corporation recommends using this script for debugging purposes only — it may affect call processing.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if matching entries are found?	Set to **y** to raise an event if the trace files contain entries that match your text string. The default is y.
Collect data?	Set to **y** to collect data about trace file entries for reports and graphs. The default is n.
Trace file directory	Specify the file path to the trace file. The default is `c:\program files\cisco\trace\ccm`.
Search for this text	Specify the text string that you want to find in the trace files. The default is `error|warning|failed|unexpected`.
On first run, scan files modified in the last N minutes	Set this parameter to determine how many minutes to go back and check for modified files the first time you run this script. Subsequent searches begin where the previous one finished. For instance, if you enter 15, the script will check for files modified within the past 15 minutes. The default is 30 minutes.
Event severity when matching entries are found	Set the event severity level, from 1 to 40,to indicate the importance of the event. The default is 25.
Maximum entries per event message	Specify the maximum number of entries that can be placed into a single event message. If more entries are found, a new event is generated. The default is 100 entries.

Transcoder_Device

Use this Knowledge Script to monitor the number of active and available resources for an individual transcoder device. This script also monitors whether the transcoder device ran out of resources at any time during the specified interval.

Resource Object

CCM Transcoder Device object

Default Schedule

By default, this script runs daily every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is exceeded or not met. The event message for an out-of-resource event contains the number of times that the device ran out of resources. The default is y.
Collect data?	Set to **y** to collect data about active and available resources for reports and graphs. The default is n.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded or not met. The default is 15.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not registered.
Threshold - Maximum active resources	Specify the maximum number of transcoder resources that can be active (in use) before an event is raised. The default is 20 resources.
Threshold - Minimum available resources	Specify the minimum number of transcoder resources that must be available to prevent an event from being raised. The default is 0 resources.
Event severity when transcoder device was out of resources	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the transcoder device ran out of resources at least once during the interval. Set to 0 to ignore an out-of-resource event. The default is 25.

TranscoderResources

A transcoder is a device that takes the output stream of one codec and transcodes (converts) it from one compression type to another compression type. In CallManager, the transcoders convert between the G.711, G.723, and G.729 codecs.

Cisco CallManager invokes a transcoder on behalf of endpoint devices when the two devices are using different codecs. When inserted into a call, the transcoder converts the data streams between the different codecs, enabling communication between them.

Use this Knowledge Script to monitor the transcoder performance counters:

- **TranscoderResourcesActive**. The total number of transcoders that are in use on all transcoder devices registered with this CallManager. A transcoder in use is one transcoder resource that has been allocated for use in a call.
- **TranscoderResourcesAvailable**. The total number of transcoders that are not in use and are available for allocation on all transcoder devices registered with this CallManager.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is exceeded or not met. The default is y.
Collect data?	Set to **y** to collect data about transcoder resources for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Event severity when threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded or not met. The default is 15.
Threshold - Maximum active transcoder resources	Specify the maximum number of transcoder resources that can be active before an event is raised. The default is 10 resources.
Threshold - Minimum available transcoder resources	Specify the minimum number of transcoder resources that must be available to prevent an event from being raised. The default is 2 resources.

TranscoderUnavailable

A transcoder is a device that takes the output stream of one codec and transcodes (converts) it from one compression type to another compression type. In CallManager, the transcoders convert between the G.711, G.723, and G.729 codecs.

Cisco CallManager invokes a transcoder on behalf of endpoint devices when the two devices are using different codecs. When inserted into a call, the transcoder converts the data streams between the different codecs, enabling communication between them.

Use this Knowledge Script to monitor the number of times that CallManager attempted to allocate a transcoder resource from one of the transcoder devices registered to this CallManager when none was available, either because all were in use or none was registered.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if transcoder resources are unavailable?	Set to **y** to raise an event. if transcoder resources are unavailable. The default is y.
Collect data?	Set to **y** to collect data about unavailable transcoder resources for reports and graphs. The default is n.
Event severity when transcoder resources are unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of unavailable resource instances exceeds the threshold. The default is 10.
Threshold - Maximum unavailable resource instances	Specify the maximum number of times that transcoder resources can be unavailable before an event is raised. The default is 0 resources.

UnicastConfActive

Use this Knowledge Script to monitor the number of active Unicast software and hardware conferences. This script raises an event if the number of active conferences exceeds the threshold.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a the number of active hardware or software conferences exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about active conferences for graphs and reports. The default is n.
Monitor active Unicast software conferences?	Set to **y** to monitor the number of active Unicast software conferences. The default is y
Threshold - Maximum active Unicast software conferences	Specify the maximum number of software conferences that can be active before an event is raised. The default is 50 conferences.
Monitor active Unicast hardware conferences?	Set to **y** to monitor the number of active Unicast hardware conferences. The default is y.
Threshold - Maximum active hardware conferences	Specify the maximum number of hardware conferences that can be active before an event is raised. The default is 50 conferences.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active hardware or software conferences exceeds the threshold. The default is 25.

UnicastConfAvailable

Use this Knowledge Script to monitor the number of new Unicast conferences that can be started. This script raises an event if the number of available hardware or software conferences falls below the threshold.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is not met?	Set to **y** to raise an event if the number of available hardware or software conferences falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about available conferences for reports and graphs. The default is n.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not actively handling calls.
Monitor available Unicast software conferences?	Set to **y** to monitor the number of available Unicast software conferences. The default is y.
Threshold - Minimum available software conferences	Specify the minimum number of software conferences that must be available to prevent an event from being raised. The default is 3 conferences.
Monitor available Unicast hardware conferences?	Set to **y** to monitor the number of available Unicast hardware conferences. The default is y.
Threshold - Minimum available hardware conferences	Specify the minimum number of hardware conferences that must be available to prevent an event from being raised. The default is 3 conferences.
Event severity when threshold is not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of available hardware or software conferences falls below the threshold. The default is 15.

UnicastConfBridge_Device

Use this Knowledge Script to monitor the number of active and available resources for an individual Unicast software or hardware conference bridge device. This script also detects whether the Unicast device ran out of resources at any time during the specified interval.

Resource Objects

CCM Unicast Software Conference Bridge object

CCM Unicast Hardware Conference Bridge object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is exceeded or not met. The default is y.
Collect data?	Set to **y** to collect data about active and available resources for graphs and reports. The default is n.
Event severity when resource threshold is breached	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a resource threshold is exceeded or not met. The default is 15.
Suppress event when Role is set to Backup?	Set to **y** to suppress event generation on CallManager resources whose role is set to "backup." The default is y. By suppressing event generation, you can run a script on all CallManager resources without raising an event on a resource that is not handling calls.
Threshold - Maximum active hardware resources	Specify the maximum number of conference bridge hardware resources that can be active (in use) before an event is raised. The default is 8 resources.
Threshold - Maximum active software resources	Specify the maximum number of conference bridge software resources that can be active (in use) before an event is raised. The default is 36 resources.
Threshold - Minimum available resources	Specify the minimum number of software and hardware resources that must be available to prevent an event from being raised. The default is 0 resources.
Monitor for active participants?	Set to n if you do not want to monitor or collect data for the number of active conference participants. The default is y.
Threshold - Maximum active participants	Specify the maximum number of participants that can be active before an event is raised. The default is 10.
Event severity when active participants exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active participants exceeds the threshold. Set to 0 to ignore an active participant event. The default is 25.

Parameter	How to Set It
Monitor for completed conferences?	Set to **n** if you do not want to monitor or collect data for the number of conferences completed during the interval. The default is y.
Threshold - Maximum completed conferences	Specify the maximum number of conferences that can have been completed since the last time this script ran. If the number of completed conferences exceeds this amount, an event is raised. The default is 20 conference. A conference is started when the first call is connected to the bridge. The conference is completed when the last call is disconnected from the bridge.
Event severity when completed conferences exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of completed conferences exceeds the threshold. Set to 0 to ignore a completed conference event. The default is 25.
Event severity when conference bridge device is out of resources	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the conference bridge device ran out of resources at least once during the interval. Set to 0 to ignore an out-of-resource event. The default is 25.

UnicastConfComplete

Use this Knowledge Script to monitor the number of Unicast conferences completed during an interval. This script raises an event if the number of completed hardware or software conferences exceeds the threshold.

The event message for the out-of-resources event contains the number of times that the device ran out of resources. Short messages, detailed event messages, and data stream headers will specify whether the device was a hardware or software conference bridge device.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if completed conferences exceed the threshold?	Set to **y** to raise an event if the number of completed hardware and software conferences exceed the threshold. The default is y.
Collect data?	Set to **y** to collect data about completed conferences for graphs and reports. The default is n.
Monitor completed Unicast software conferences?	Set to **y** to monitor the number of completed Unicast software conferences. The default is y.
Threshold - Maximum completed software conferences	Specify the maximum number of software conferences that can be completed before an event is raised. The default is 50 conferences.
Monitor completed Unicast hardware conferences?	Set to **y** to monitor the number of completed Unicast hardware conferences. The default is y.
Threshold - Maximum completed hardware conferences	Set the threshold for the most hardware conferences that can be completed before an event is raised. The default is 50 conferences.
Event severity when completed conferences exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of completed hardware and software conferences exceed the threshold. The default is 25.

UnicastConfParticipants

Use this Knowledge Script to monitor the number of active Unicast participants. This script raises an event if the number of active software or hardware participants exceeds a threshold.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if active participants exceed threshold?	Set to **y** to raise an event if the number of active software or hardware participants exceed a threshold. The default is y.
Collect data?	Set to **y** to collect data about active participants for graphs and reports. The default is n.
Monitor active Unicast software participants?	Set to **y** to monitor the number of active Unicast software participants. The default is y.
Threshold - Maximum active software participants	Specify the maximum number of software participants that can be active before an event is raised. The default is 100 participants.
Monitor active Unicast hardware participants?	Set to **y** to monitor the number of active Unicast hardware participants. The default is y.
Threshold - Maximum active hardware participants	Specify the maximum number of hardware participants that can be active before an event is raised. The default is 100 participants.
Event severity when active participants exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active software or hardware participants exceeds a threshold. The default is 25.

UnicastConfUnavailable

Use this Knowledge Script to monitor the number of times during an interval that a Unicast conference resource was requested when none was available. This script raises an event if the number exceeds the threshold.

Resource Object

CCM Call Processor

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of unavailable resource instances exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about unavailable resources for graphs and reports. The default is n.
Monitor Unicast software conference unavailable resource instances?	Set to **y** to monitor the number of times that a Unicast software conference resource was unavailable. The default is y.
Threshold - Maximum software unavailable resource instances	Specify the maximum number of times that a software conference resource can be unavailable before an event is raised. The default is 0.
Monitor Unicast hardware conference unavailable resource instances?	Set to **y** to monitor the number of times that a Unicast hardware conference resource was unavailable. The default is y.
Threshold - Maximum hardware unavailable resource instances	Specify the maximum number of times that a hardware conference resource can be unavailable before an event is raised. The default is 0.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of unavailable resource instances exceeds the threshold. The default is 5.

VerifyPasswords

Use this Knowledge Script to verify the sa, Administrator, and Directory Manager passwords on a CallManager computer. Cisco CallManager requires these passwords to be the same for all computers in a cluster. You can run this script daily to monitor whether any password has changed. This script raises an event if a password cannot be verified.

Reasons other than an invalid password can prevent this script from verifying the password, such as services being down or connection failures.

Resource Object

CCM parent object

Default Schedule

By default, this script runs every 24 hours.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if any verification fails or if all verifications succeed?	Set to **y** to raise an event if any password verification fails or if all verifications succeed. The default is y.
Event severity when any verification fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which any password verification attempt fails. The default is 15.
Event severity when all verifications succeed	Set the severity level, from 1 to 40, to indicate the importance of an event in which all password verification attempts succeed. Accept the default of **0** if you do not want to raise an event for this scenario.
Windows username	Provide the name of the Windows user whose password you want to verify. Leave this parameter blank to skip Windows verification. The default is Administrator.
Windows password	Provide the Windows password that you want to verify.
Domain name	Specify the domain name of the Windows user whose password you want to verify. Leave this parameter blank to use the name of the computer on which the script will be running. This parameter is optional if you are verifying a Windows password.
SQL username	Provide the user login account required to access the SQL Server database. Configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**. Leave this parameter blank to skip SQL verification. The default is sa.
SQL password	SPecify the SQL password that you want to verify.

Parameter	How to Set It
SQL Server name	Specify the name of the server where the user is to be verified. Leave this parameter blank to use the name of the computer on which the script will be running. This parameter is optional if you are verifying a SQL password.
SQL database name	Specify the name of the database for which the SQL password is to be verified. The default is master.
DC Directory username	SPecify the name of the DC Directory (LDAP) user whose password you want to verify. Leave this parameter blank to skip DC Directory verification. The default is Directory Manager.
DC Directory password	SPecify the DC Directory password that you want to verify.

Recommended Knowledge Script Groups

The several CiscoCallMgr Knowledge Scripts are members of recommended Knowledge Script Groups (KSG). The parameters of all scripts in the KSG are set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and run the KSG on a CallManager resource.

NetIQ Corporation does not recommend you run large numbers of jobs all at the same time on one CallManager system. Running a large numbers of jobs that are collecting data and running at frequent intervals may impact the performance of the CallManager server. The Knowledge Scripts in the KSGs are optimized to run continually on CallManager systems with minimal performance impact.

The KSGs provide a "best practices" usage of AppManager for monitoring your CallManager environment. You can use these KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView. For more information, see "About Policy-Based Monitoring" in the AppManager Help.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the CiscoCallMgr tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoCallMgr tab are not affected.

When deployed as part of a KSG, a script's default script parameter settings may differ from when the script is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the KSGs and want to restore it to its original form, you can reinstall the AppManager for Cisco CallManager module on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\CiscoCallMgr\RECOMMENDED` directory.

Monitoring Scripts

You can find these scripts in a the **CiscoCallMgr** group on the RECOMMENDED tab of the Knowledge Script pane, or individually on the CiscoCallMgr tab.

- CallActivity
- CallsInProgress
- LossOfHardwarePhones
- CCM_HealthCheck
- CCM_HeartBeat
- CCM_RoleStatus
- CCM_SystemUsage
- CCM_WebPageCheck
- CiscoBackupStatus
- SQL_DBGrowthRate
- SQL_NearFileMaxSize
- SQL_RepTransactions
- TftpHeartBeat
- TftpRequests

Report Scripts

You can find these scripts in a the **CiscoCallMgr_Reports** group on the RECOMMENDED tab of the Knowledge Script pane, or individually on the CiscoCallMgr tab.

- Report_CallActivity
- Report_CallsByHour
- Report_ServicesAvailability
- Report_SystemUsage

Chapter 19
CiscoCM Knowledge Scripts

AppManager for Cisco Unified Communications Manager provides the following Knowledge Scripts for monitoring a Unified Communications Manager environment.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
4x_PhoneDeregistrations	Monitors phone deregistrations on a Communications Manager 4.x cluster and maintains a history of deregistrations in the Cisco CM supplemental database.
4x_RetrieveConfigData	Retrieves Communications Manager 4.x configuration data and stores it the Cisco CM supplemental database.
4x_SetupSupplementalDB	Creates a Cisco CM supplemental database in which to store Communications Manager 4.x configuration and phone deregistration information.
AnalogAccess_GatewayUsage	Monitors resource usage for analog access gateways.
Annunciator_Device	Monitors resource usage for annunciator devices.
AttendantConsole	Monitors activity for the Attendant Console application.
CCM_CallActivity	Monitors call activity on a Communications Manager server.
CCM_MediaResources	Monitors media resources for a Communications Manager.
CCM_MGCPResources	Monitors active MGCP gateway resource usage for a Communications Manager.
CCM_RegisteredResources	Monitors changes in the number of resources registered to a Communications Manager server.
CCM_ResourceAvailability	Monitors the number of times Communications Manager requests a resource that is unavailable.
CCM_SystemPerformance	Monitors call throttling and signal processing queues for a Communications Manager.
CDR_CallFailures	Monitors call detail records retrieved from Communications Manager for calls that ended with an abnormal termination code.
CDR_CallQuality	Monitors call detail records and call management records retrieved from Communications Manager for jitter, latency, lost data, and MOS.
CDR_Query	Queries call detail records retrieved from Communications Manager and stored in the Cisco CM supplemental database.
CDR_RetrieveCallRecords	Retrieves call detail records from Communications Manager and places them in the Cisco CM supplemental database.

Knowledge Script	What It Does
CDR_RetrieveConfigData	Retrieves Communications Manager configuration data and stores it the Cisco CM supplemental database.
CFB_Hardware_Device	Monitors the resource usage of registered hardware conference bridge devices.
CFB_Software_Device	Monitors the resource usage of registered software conference bridge devices.
CFB_Video_Device	Monitors the resource usage of registered video conference bridge devices.
CTIManager	Monitors the usage of the Communications Manager CTI Manager.
ExtensionMobility	Monitors activity for the Extension Mobility application.
GatekeeperActivity	Monitors the activity on a gatekeeper.
GeneralCounter	Monitors a user-specified Performance Monitor counter.
H323_Gateway_CallActivity	Monitors call activity for H323 gateway devices.
H323_Trunk_CallActivity	Monitors call activity for H323 trunk devices.
HealthCheck	Monitors the operational status of active services on Communications Manager servers.
HuntAndRouteList	Monitors hunt lists and route lists for availability and call activity.
Locations	Monitors Cisco locations for voice and video bandwidth availability and usage.
MediaStreamingApp	Monitors the resources handled by the Media Streaming Application.
MGCP_FXO_CallActivity	Monitors completed calls, blocked calls, outbound busy attempts, and port status on MGCP FXO devices.
MGCP_FXS_CallActivity	Monitors completed calls, blocked calls, outbound busy attempts, and port status on MGCP FXS devices.
MGCP_GatewayUsage	Monitors active and in-service ports, active channels, and in-service spans for MGCP gateways.
MGCP_PRI_CallActivity	Monitors completed calls, outbound busy attempts, active calls, blocked calls, and data link availability for MGCP PRI devices.
MGCP_PRI_ChannelHealth	Monitors the status of channels for MGCP PRI devices.
MGCP_T1CAS_CallActivity	Monitors completed calls, outbound busy attempts, active calls, and blocked calls for MGCP T1CAS devices.
MGCP_T1CAS_ChannelHealth	Monitors the status of channels for an MGCP T1CAS device.
MOH_Device	Monitors the resource usage for a registered Music-on-Hold device.
MTP_Device	Monitors the resource usage for a registered Media Termination Point device.
PhoneDeregistrations	Monitors phone deregistrations for a Communications Manager and retains deregistration history in the Cisco CM supplemental database.
PhoneInventory	Creates an inventory of the phones configured in a Communications Manager cluster.
Report_PhoneDeregAudit	Creates a history of phone deregistrations and reregistrations.
Report_PhoneDeregWatchList	Creates a list of phones that frequently deregister.
RoleStatus	Monitors status changes for primary and backup Communications Managers in a Communications Manager group.

Knowledge Script	What It Does
SetupSupplementalDB	Creates a Cisco CM supplemental database in which to store Communications Manager call detail records.
SIP_Trunk_CallActivity	Monitors call activity for SIP trunk devices.
SNMPTrap_AddMIB	Add management information bases for monitoring by the SNMPTrap_Async Knowledge Script.
SNMPTrap_Async	Checks for incoming SNMP traps forwarded from NetIQ SNMP Trap Receiver.
SystemUpTime	Monitors the number of hours Communications Manager has been operational since its last reboot.
SystemUsage	Monitors CPU, memory, and disk usage for a Communications Manager server.
TFTPActivity	Monitors activity on the Cisco TFTP server.
Transcoder_Device	Monitors the resources used by registered transcoder devices.
WebDialer	Monitors activity for the Cisco Web Dialer application.
WebPageCheck	Monitors the availability of and round-trip time to the ccmadmin and ccmuser Web pages.
Recommended Knowledge Script Group	Performs essential monitoring of your Cisco Unified Communications Manager environment.

4x_PhoneDeregistrations

Use this Knowledge Script to monitor phone deregistrations on a Communications Manager 4.x cluster and to maintain a history of deregistrations in the Cisco CM supplemental database. This script raises an event if the number or percentage of lost phones exceeds the threshold you set. You determine how long a phone must be deregistered before it is considered "lost." In addition, you determine whether to group events by cluster, device pool, location, or partition.

Prerequisites

Run the 4x_SetupSupplementalDB Knowledge Script to create the Cisco CM supplemental database. Then, run the 4x_RetrieveConfigData Knowledge Script to retrieve Communications Manager 4.x configuration information.

Resource Object

CiscoCM_Cluster4xMgmt

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the 4x_PhoneDeregistration job. The default is 5.
Event Notification	
Raise event if lost phones in group exceed threshold?	Select **Yes** to raise an event if the number or percentage of lost phones in a group exceeds the threshold you set. The default is Yes. Use *Select event grouping* to select how to group the lost phones. Use *Maximum time phone deregistered before counted as lost* to determine how long a phone must be deregistered before it is considered lost.
Select event grouping	Select whether to group lost phones by **Cluster**, **Device Pool**, **Location**, or **Partition**. AppManager raises an event based on whether the number of lost phones in *each* group exceeds the threshold you set. For example, you set *Maximum number of lost phones in the group* to 5, you set *Select event grouping* to Device Pool, and you have three device pools. If AppManager detects six lost phones in the first pool, two in the second, and seven in the third, it will raise two events: one for the six lost phones in the first pool and another for the seven lost phones in the third pool. Because you set the threshold to "5," no event is raised for the lost phones in the second pool. The default is Cluster.

Parameter	How to Set It
Maximum time phone deregistered before counted as lost	Specify the number of minutes that must elapse before a deregistered phone can be considered a “lost” phone. The default is 0 minutes. Accept the default if you want *all* deregistered phones to be considered lost.
Type of threshold	Select whether you want to raise events based on the **Number** or **Percent** of lost phones. The default is Number.
Threshold - Maximum number of lost phones	Use this parameter if you selected **Number** in *Type of threshold*. Specify the maximum number of phones that can be lost before an event is raised. The default is 0.
Threshold - Maximum percent of lost phones	Use this parameter if you selected **Percent** in *Type of threshold*. Specify the maximum percentage of phones that can be lost before an event is raised. The default is 0.
Event severity when lost phones exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number or percentage of lost phones in a group exceeds the threshold you set. The default is 15.
Include lost phone details in event message	Select **Yes** to include details of the lost phones in the event message. Phone details can include device name, device IP address, directory number, description, name of device pool, time of deregistration, and the Communications Manager from which the phone was deregistered. The default is Yes.
Maximum number of detail rows to include in event detail	Specify the maximum number of detail rows to include in an event message. Each row contains details for one phone. Rows are sorted in order by most recently lost phone. Specify “0” to include all rows. The default is 20. This parameter is applicable only if you selected **Yes** for *Include lost phone details in event message*.

4x_RetrieveConfigData

Use this Knowledge Script to retrieve Communications Manager configuration data from the Communications Manager 4.x Publisher and store it in the Cisco CM supplemental database.

Prerequisite

Run the 4x_SetupSupplementalDB Knowledge Script to create the Cisco CM supplemental database.

Resource Object

CiscoCM_Cluster4xMgmt

Default Schedule

By default, this script runs once a day, at 3 A.M, so as to perform its possibly CPU-intensive function at a time when the Communications Manager is least busy.

However, because the 4x_PhoneDeregistrations script uses the configuration data this script retrieves, you may want to set this script to "Run Once" so the configuration data is retrieved immediately. Once the "Run Once" job is complete, you can then run this script using the default schedule of once daily.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the 4x_RetrieveConfigData job. The default is 5.
Raise event if configuration retrieval succeeds?	Select **Yes** to raise an event if Communications Manager 4.x configuration data is successfully retrieved from the Cisco CM supplemental database. The default is unselected.
Event severity when configuration retrieval succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which configuration data is successfully retrieved from the Cisco CM supplemental database. The default is 25.

4x_SetupSupplementalDB

Use this Knowledge Script to create a Cisco CM supplemental database in which to store Communications Manager 4.x phone deregistration information.

Resource Object

CiscoCM_Cluster4xMgmt

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the 4x_SetupSupplementalDB job. The default is 5.
Raise event if database setup succeeds?	Select **Yes** to raise an event if the Cisco CM supplemental database is successfully created on the proxy agent computer. The default is unselected.
Event severity when database setup succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Cisco CM supplemental database is successfully created. The default is 25.
Phone Deregistration Parameters	
Number of days to keep phone deregistration audit entries	Specify the number of days' worth of phone deregistration audit entries you want to keep in the Cisco CM supplemental database. Any data older than what you specify is discarded. The default is 180 days.
Is your CallManager configured to use secure Web access (HTTPS)?	Select **Yes** if you use secure HTTP (HTTPS) to access your Communications Manager. AppManager uses this information to build the Communications Manager URL that is displayed in event message details. The default is unselected.
SQL Server Information	
Local SQL Server Instance name	Specify the name of the local SQL Server instance (on the proxy agent computer) in which you want to create the new Cisco CM supplemental database. Leave this parameter blank to accept the default name.

AnalogAccess_GatewayUsage

Use this Knowledge Script to monitor active ports, out-of-service ports, and outbound busy attempts for analog access gateways. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for active ports, out-of-service ports, and outbound busy attempts.

Resource Object

CiscoCM_AnalogAccessObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the AnalogAccess_GatewayUsage job. The default is 5.
Monitor Active Ports	
Event Notification	
Raise event if active ports exceed threshold?	Select **Yes** to raise an event if the number of active ports exceeds the threshold you set. The default is Yes.
Threshold - Maximum active ports	Specify the maximum number of ports that can be active before an event is raised. The default is 20 ports.
Event severity when active ports exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active ports exceeds the threshold. The default is 15.
Data Collection	
Collect data for active ports?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of ports that are active at each script iteration.
Monitor Busy Attempts	
Event Notification	
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of times that the gateway received a busy signal exceeds the threshold you set. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of times the gateway can attempt a connection that receives a busy signal before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold. The default is 15.
Data Collection	
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of gateway connection attempts that received a busy signal during the monitoring period.

Parameter	How to Set It
Monitor Out of Service Ports	
Event Notification	
Raise event if out of service ports exceed threshold?	Select **Yes** to raise an event if the number of ports that were out of service exceeds the threshold you set. The default is Yes.
Threshold - Maximum out of service ports	Specify the maximum number of ports that must be out of service before an event is raised. The default is 0 ports.
Event severity when out of service ports exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of out-of-service ports exceeds the threshold. The default is 15.
Data Collection	
Collect data for out of service ports?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of ports that are out of service at each script iteration.

Annunciator_Device

Use this Knowledge Script to monitor the annunciator resource usage for a Communications Manager. An annunciator enables Communications Manager to play recorded announcements and tones to Cisco IP phones, gateways, and other configurable devices.

This script raises an event if the number of times annunciator resources were unavailable exceeds the threshold, or if the percentage of resource usage exceeds the threshold. In addition, this script generates data streams for the number of active resources, the number of available resources, the number of times resources were unavailable, and the percentage of resource usage.

Resource Object

CiscoCM_AnnunciatorObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Annunciator_Device job. The default is 5.
Monitor Resource Usage	
Event Notification	
Raise event if resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of annunciator resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum resource usage	Specify the highest percentage of annunciator resource usage that must be detected before an event is raised. The default is 80%.
Event severity when resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which annunciator resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of annunciator resource usage at each script iteration.
Monitor Active Resources	
Data Collection	
Collect data for active resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of annunciator resources that are active at each script iteration.
Monitor Available Resources	
Data Collection	

Parameter	How to Set It
Collect data for available resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of annunciator resources that are available at each script iteration.
Monitor Unavailable Resources	
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times that annunciator resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times annunciator resources must be unavailable before an event is raised. The default is 0 instances.
Event severity when number of times resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times annunciator resources were unavailable exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times annunciator resources were unavailable during the monitoring period.

AttendantConsole

Use this Knowledge Script to monitor handled and in-progress requests for the Attendant Console application. Attendant Console allows you to set up Cisco IP phones to use speed-dial buttons and quick directory access, look up phone numbers, monitor line status, and redirect calls.

This script raises an event if the number of redirected calls and online clients exceed the threshold you set. In addition, this script generates data streams for the number of redirected calls, the number of total calls, the number of online clients, the number of registered clients, and the line connection state.

Resource Object

CiscoCM_AttendConsole

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the AttendantConsole job. The default is 5.
Monitor Redirected Calls	
Event Notification	
Raise event if redirected calls exceed threshold?	Select **Yes** to raise an event if the number of redirected calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum redirected calls	Specify the maximum number of calls that must be redirected before an event is raised. The default is 50 calls.
Event severity when redirected calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of redirected calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for redirected calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were redirected during the monitoring period.
Monitor Total Calls	
Data Collection	
Collect data for total calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of calls handled by Attendant Console during the monitoring period.
Monitor Online Clients	
Event Notification	

Parameter	How to Set It
Raise event if online clients exceed threshold?	Select **Yes** to raise an event if the number of online clients exceeds the threshold you set. The default is Yes.
Threshold - Maximum online clients	Specify the maximum number of clients that must be online before an event is raised. The default is 100 clients.
Event severity when online clients exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of online clients exceeds the threshold. The default is 15.
Data Collection	
Collect data for online clients?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of clients that are online at each script iteration.
Monitor Registered Clients	
Data Collection	
Collect data for registered clients?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of clients that are registered at each script iteration.
Monitor Connection State	
Data Collection	
Collect data for connection state?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the line connection state for the Cisco Telephony Call Dispatcher (TCD) at each script iteration. Attendant Console uses TCD for login services, line state, and directory services. There are four line connection states: • 0 - Not registered or not receiving line link state information from Communications Manager • 1 - Registered and receiving line link state information from Communications Manager • 10 - TCD is logged in, but has not registered or received line link state information from Communications Manager • 11 - TCD is logged in, has registered, and is receiving line link state information from Communications Manager

CCM_CallActivity

Use this Knowledge Script to monitor call activity on a Communications Manager server. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following metrics:

- Attempted calls
- Completed calls
- Active calls
- In-progress calls
- Incomplete calls (%)
- Attempted system calls
- Completed video calls

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 1172.

Resource Object

CiscoCM_CMServer

Default Schedule

By default, this script runs every five minutes.

If you are running this script as part of the recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CCM_CallActivity job. The default is 5.
Monitor Attempted Calls	
Event Notification	
Raise event if attempted calls exceed threshold?	Select **Yes** to raise an event if the number of attempted calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum attempted calls	Specify the maximum number of calls that must be attempted before an event is raised. The default is 500 calls.
Event severity when attempted calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of attempted calls exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for attempted calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were attempted during the monitoring period. The default is Yes.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were completed during the monitoring period. The default is Yes.
Monitor Active Calls	
Data Collection	
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that are active at each script iteration. The default is Yes. A call is considered “active” once a connection is made.
Monitor Calls in Progress	
Event Notification	
Raise event if calls in progress exceed threshold?	Select **Yes** to raise an event if the number of in-progress calls exceeds the threshold you set. The default is Yes. A call is considered “in-progress” as soon as the receiver is lifted.
Threshold - Maximum calls in progress	Specify the maximum number of calls that must be in progress before an event is raised. The default is 1000 calls.
Event severity when calls in progress exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-progress calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for calls in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls in progress at each script iteration. The default is Yes.
Monitor Incomplete Calls	
Event Notification	
Raise event if incomplete calls exceeds threshold?	Select **Yes** to raise an event if the percentage of incomplete calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum incomplete calls	Specify the highest percentage of incomplete calls that must be detected before an event is raised. The default is 80%.
Event severity when incomplete calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of incomplete calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for percent incomplete calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of incomplete calls during the monitoring period. The default is Yes.
Monitor Attempted System Calls	
Event Notification	
Raise event if attempted system calls exceed threshold?	Select **Yes** to raise an event if the number of attempted system calls exceeds the threshold you set. The default is Yes. System calls are signals sent to phones to turn on/off the Message Waiting indicator. A system call is sent to illuminate the indicator when a message is left, and another one is sent to turn off the indicator when the user listens to that message.

Parameter	How to Set It
Threshold - Maximum attempted system calls	Specify the highest number of system calls that must be attempted before an event is raised. The default is 500 calls.
Event severity when attempted system calls calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of attempted system calls exceeds the threshold. The default is 25.
Data Collection	
Collect data for attempted system calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of system calls attempted during the monitoring period. The default is Yes.
Monitor Completed Video Calls	
Data Collection	
Collect data for completed video calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of video calls that were completed during the monitoring period. The default is Yes.

CCM_MediaResources

Use this Knowledge Script to monitor Communications Manager media resources:

- Annunciators
- Conference bridges
- Music-on-Hold (MOH)
- Media Termination Points (MTP)
- Transcoders

This script raises an event if a threshold is exceeded. In addition, this script generates percentage and active data streams for annunciator resource usage, conference bridge resource usage (application-controlled, hardware, software, and video), MTP resource usage, MOH (unicast and multicast) resource usage, and transcoder resource usage.

Resource Object

CiscoCM_CallProcessor

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CCM_MediaResources job. The default is 5.
Monitor Annunciator Resource Usage	
Event Notification	
Raise event if annunciator resource usage exceeds threshold?	Select **Yes** to raise an event if annunciator resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum annunciator resource usage	Specify the maximum percentage of annunciator resource usage that must be detected before an event is raised. The default is 90%.
Event severity when annunciator resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which annunciator resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for annunciator resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of annunciator resource usage at each script iteration.
Monitor Application Controlled Bridge Resource Usage	
Event Notification	

Parameter	How to Set It
Raise event if application controlled bridge resource usage exceeds threshold?	Select **Yes** to raise an event if application-controlled bridge resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum application controlled bridge resource usage	Specify the maximum percentage of application-controlled bridge resource usage that must be detected before an event is raised. The default is 90%.
Event severity when application controlled bridge resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which application-controlled bridge resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for application controlled bridge resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of application-controlled bridge resource usage at each script iteration.
Monitor Hardware Conference Bridge Resource Usage	
Event Notification	
Raise event if hardware conference bridge resource usage exceeds threshold?	Select **Yes** to raise an event if hardware conference bridge resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum hardware conference bridge resource usage	Specify the maximum percentage of hardware conference bridge resource usage that must be detected before an event is raised. The default is 90%.
Event severity when hardware conference bridge resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which hardware conference bridge resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for hardware conference bridge resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of hardware conference bridge resource usage at each script iteration.
Monitor Software Conference Bridge Resource Usage	
Event Notification	
Raise event if software conference bridge resource usage exceeds threshold?	Select **Yes** to raise an event if software conference bridge resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum software conference bridge resource usage	Specify the maximum percentage of software conference bridge resource usage that must be detected before an event is raised. The default is 90%.
Event severity when software conference bridge resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which software conference bridge resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for software conference bridge resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of software conference bridge resource usage at each script iteration.

Parameter	How to Set It
Monitor Video Conference Bridge Resource Usage	
Event Notification	
Raise event if video conference bridge resource usage exceeds threshold?	Select **Yes** to raise an event if video conference bridge resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum video conference bridge resource usage	Specify the maximum percentage of video conference bridge resource usage that must be detected before an event is raised. The default is 90%.
Event severity when video conference bridge resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which video conference bridge resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for video conference bridge resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of video conference bridge resource usage at each script iteration.
Monitor Media Termination Point Resource Usage	
Event Notification	
Raise event if Media Termination Point resource usage exceeds threshold?	Select **Yes** to raise an event if MTP resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum Media Termination Point resource usage	Specify the maximum percentage of MTP resource usage that must be detected before an event is raised. The default is 90%.
Event severity when Media Termination Point resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MTP resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for Media Termination Point resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of MTP resource usage at each script iteration.
Monitor Music-on-Hold Multicast Resource Usage	
Event Notification	
Raise event if Music-on-Hold multicast resource usage exceeds threshold?	Select **Yes** to raise an event if MOH multicast resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum Music-on-Hold multicast resource usage	Specify the maximum percentage of MOH multicast resource usage that must be detected before an event is raised. The default is 90%.
Event severity when Music-on-Hold multicast resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MOH multicast resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for Music-on-Hold multicast resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of MOH multicast resource usage at each script iteration.

Parameter	How to Set It
Monitor Music-on-Hold Unicast Resource Usage	
Event Notification	
Raise event if Music-on-Hold unicast resource usage exceeds threshold?	Select **Yes** to raise an event if MOH unicast resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum Music-on-Hold unicast resource usage	Specify the maximum percentage of MOH unicast resource usage that must be detected before an event is raised. The default is 90%.
Event severity when Music-on-Hold unicast resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MOH unicast resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for Music-on-Hold unicast resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of MOH unicast resource usage at each script iteration.
Monitor Transcoder Resource Usage	
Event Notification	
Raise event if transcoder resource usage exceeds threshold?	Select **Yes** to raise an event if transcoder resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum transcoder resource usage	Specify the maximum percentage of transcoder resource usage that must be detected before an event is raised. The default is 90%.
Event severity when transcoder resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which transcoder usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for transcoder resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of transcoder resource usage at each script iteration.
Monitor Active Annunciator Resources	
Data Collection	
Collect data for active annunciator resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of annunciator resources that are active at each script iteration.
Monitor Active Application Controlled Bridge Resources	
Data Collection	
Collect data for active application-controlled bridge resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of application-controlled bridge resources that are active at each script iteration.
Monitor Active Hardware Conference Resources	
Data Collection	
Collect data for active hardware conference resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of hardware conference resources that are active at each script iteration.
Monitor Active Software Conference Resources	
Data Collection	

Parameter	How to Set It
Collect data for active software conference resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of software conference resources that are active at each script iteration.
Monitor Active Video Conference Resources	
Data Collection	
Collect data for active video conference resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of video conference resources that are active at each script iteration.
Monitor Active Media Termination Point Resources	
Data Collection	
Collect data for active Media Termination Point resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MTP resources that are active at each script iteration.
Monitor Active Music-on-Hold Multicast Resources	
Data Collection	
Collect data for active Music-on-Hold multicast resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MOH multicast resources that are active at each script iteration.
Monitor Active Music-on-Hold Unicast Resources	
Data Collection	
Collect data for active Music-on-Hold unicast resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MOH unicast resources that are active at each script iteration.
Monitor Active Transcoder Resources	
Data Collection	
Collect data for active transcoder resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of transcoder resources that are active at each script iteration.

CCM_MGCPResources

Use this Knowledge Script to monitor active and in-service MGCP gateway resource usage for a Communications Manager:

- BRI (basic rate interface) channels and spans
- FXO (foreign exchange office) ports
- FXS (foreign exchange station) ports
- PRI (primary rate interface) channels and spans
- T1CAS (channel associated signaling) channels and spans

An *active* resource is currently handling a call. An *in-service* resource is available to handle a call.

This script raises an event if any threshold is exceeded. In addition, this script generates data streams for active and in-service ports/channels/spans for any monitored resources.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 1172.

Resource Object

CiscoCM_CallProcessor

Default Schedule

By default, this script runs every ten minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CCM_MGCPResources job. The default is 5.
Monitor Active BRI Channels	
Event Notification	
Raise event if active BRI channels exceed threshold?	Select **Yes** to raise an event if the number of active BRI channels exceeds the threshold you set. The default is Yes.
Threshold - Maximum active BRI channels	Specify the maximum number of BRI channels that must be active before an event is raised. The default is 100 channels.
Event severity when active BRI channels exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active BRI channels exceeds the threshold. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for active BRI channels?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of BRI channels that are active at each script iteration. The default is Yes.
Monitor BRI Spans in Service	
Data Collection	
Collect data for BRI spans in service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of BRI spans that are in service at each script iteration. The default is Yes.
Monitor Active FXO Ports	
Event Notification	
Raise event if active FXO ports exceed threshold?	Select **Yes** to raise an event if the number of active FXO ports exceeds the threshold you set. The default is Yes.
Threshold - Maximum active FXO ports	Specify the maximum number of FXO ports that must be active before an event is raised. The default is 100 ports.
Event severity when active FXO ports exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active FXO ports exceeds the threshold. The default is 15.
Data Collection	
Collect data for active FXO ports?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of FXO ports that are active at each script iteration. The default is Yes.
Monitor FXO Ports in Service	
Data Collection	
Collect data for FXO ports in service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of FXO ports that are in service at each script iteration. The default is Yes.
Monitor Active FXS Ports	
Event Notification	
Raise event if active FXS ports exceed threshold?	Select **Yes** to raise an event if the number of active FXS ports exceeds the threshold you set. The default is Yes.
Threshold - Maximum active FXS ports	Specify the maximum number of FXS ports that must be active before an event is raised. The default is 100 ports.
Event severity when active FXS ports exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active FXS ports exceeds the threshold. The default is 15.
Data Collection	
Collect data for active FXS ports?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of FXS ports that are active at each script iteration. The default is Yes.
Monitor FXS Ports in Service	
Data Collection	
Collect data for FXS ports in service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of FXS ports that are in service at each script iteration. The default is Yes.
Monitor Active PRI Channels	
Event Notification	

Parameter	How to Set It
Raise event if active PRI channels exceed threshold?	Select **Yes** to raise an event if the number of active PRI channels exceeds the threshold you set. The default is Yes.
Threshold - Maximum active PRI channels	Specify the maximum number of PRI channels that must be active before an event is raised. The default is 250 channels.
Event severity when active PRI channels exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active PRI channels exceeds the threshold. The default is 15.
Data Collection	
Collect data for active PRI channels?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of PRI channels that are active at each script iteration. The default is Yes.
Monitor PRI Spans in Service	
Data Collection	
Collect data for PRI spans in service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of PRI spans that are in service at each script iteration. The default is Yes.
Monitor Active T1CAS Channels	
Event Notification	
Raise event if active T1CAS channels exceed threshold?	Select **Yes** to raise an event if the number of active T1CAS channels exceeds the threshold you set. The default is Yes.
Threshold - Maximum active T1CAS channels	Specify the maximum number of T1CAS channels that must be active before an event is raised. The default is 250 channels.
Event severity when active T1CAS channels exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active T1CAS channels exceeds the threshold. The default is 15.
Data Collection	
Collect data for active T1CAS channels?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of T1CAS channels that are active at each script iteration. The default is Yes.
Monitor T1CAS Spans in Service	
Data Collection	
Collect data for T1CAS spans in service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of T1CAS spans that are in service at each script iteration. The default is Yes.

CCM_RegisteredResources

Use this Knowledge Script to monitor changes in the number of resources (phones, gateways, and station devices) registered to a Communications Manager server. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the percentage of increase or decrease in registered resources, as well as data streams for the *number* of registered resources related to those percentages of increases or decreases.

If the number of registered resources increases from zero to a larger number, this script reports the increase as 100% multiplied by the number of new registered resources. For example, if the previous number of registered gateways is zero, and the latest iteration of this script finds seven new registered gateways, then the script reports the increase in registered gateways as 700%.

For more information, see PhoneInventory.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 1172.

Resource Object

CiscoCM_CMServer

Default Schedule

By default, this script runs every five minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CCM_RegisteredResources job. The default is 5.
Monitor Registered Hardware Phones	
Data Collection	
Collect data for registered hardware phones?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number hardware phones that are registered at each script iteration.
Monitor Increase in Registered Hardware Phones	
Event Notification	
Raise event if increase in registered hardware phones exceeds threshold?	Select **Yes** to raise an event if the increase in registered hardware phones exceeds the threshold you set. The default is unselected.

Parameter	How to Set It
Threshold - Maximum increase in registered hardware phones	Specify the maximum increase in the number of registered hardware phones that can occur before an event is raised. The default is 1 phone.
Event severity when increase in registered hardware phones exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of new registered hardware phones exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for increase in registered hardware phones?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of increase in hardware phones during the monitoring period. The default is unselected.
Monitor Percentage Increase in Registered Hardware Phones	
Event Notification	
Raise event if percentage increase in registered hardware phones exceeds threshold?	Select **Yes** to raise an event if the percentage increase in registered hardware phones exceeds the threshold you set. The default is Yes.
Threshold - Maximum percentage increase in registered hardware phones	Specify the maximum decrease in registered hardware phones that can occur before an event is raised. The default is 10%.
Event severity when percentage increase in registered hardware phones exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in registered hardware phones exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for decrease in registered hardware phones?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in hardware phones during the monitoring period. The default is unselected.
Monitor Decrease in Registered Hardware Phones	
Event Notification	
Raise event if decrease in registered hardware phones exceeds threshold?	Select **Yes** to raise an event if the decrease in registered hardware phones exceeds the threshold you set. The default is unselected.
Threshold - Maximum decrease in registered hardware phones	Specify the maximum decrease in the number of registered hardware phones that can occur before an event is raised. The default is 1 phone.
Event severity when decrease in registered hardware phones exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the decrease in number of registered hardware phones exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for decrease in registered hardware phones?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the decreasing number of registered hardware phones during the monitoring period.
Monitor Percentage Decrease in Registered Hardware Phones	
Event Notification	

Parameter	How to Set It
Raise event if percentage decrease in registered hardware phones exceeds threshold?	Select **Yes** to raise an event if the percentage decrease in registered hardware phones exceeds the threshold you set. The default is Yes.
Threshold - Maximum percentage decrease in registered hardware phones	Specify the maximum percentage decrease in registered hardware phones that can occur before an event is raised. The default is 10%.
Event severity when percentage decrease in registered hardware phones exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of decrease in registered hardware phones exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for percentage decrease in registered hardware phones?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in hardware phones during the monitoring period. The default is unselected.
Monitor Registered MGCP Gateways	
Data Collection	
Collect data for registered MGCP gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MGCP gateways registered at each script iteration.
Monitor Increase in Registered MGCP Gateways	
Event Notification	
Raise event if increase in registered MGCP gateways exceeds threshold?	Select **Yes** to raise an event if the increase in registered MGCP gateways exceeds the threshold you set. The default is Yes.
Threshold - Maximum increase in registered MGCP gateways	Specify the maximum increase in registered MGCP gateways that can occur before an event is raised. The default is 10%.
Event severity when increase in registered MGCP gateways exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in registered MGCP gateways exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for increase in registered MGCP gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of increase in registered MGCP gateways during the monitoring period.
Monitor Decrease in Registered MGCP Gateways	
Event Notification	
Raise event if decrease in registered MGCP gateways exceeds threshold?	Select **Yes** to raise an event if the decrease in registered MGCP gateways exceeds the threshold you set. The default is Yes.
Threshold - Maximum decrease in registered MGCP gateways	Specify the maximum decrease in registered MGCP gateways that can occur before an event is raised. The default is 10%.
Event severity when decrease in registered MGCP gateways exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of decrease in registered MGCP gateways exceeds the threshold you set. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for decrease in registered MGCP gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in registered MGCP gateways during the monitoring period.
Monitor Registered Analog Access Gateways	
Data Collection	
Collect data for registered Analog Access gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of Analog Access gateways registered at each script iteration.
Monitor Increase in Registered Analog Access Gateways	
Event Notification	
Raise event if increase in registered Analog Access gateways exceeds threshold?	Select **Yes** to raise an event if the increase in registered Analog Access gateways exceeds the threshold you set. The default is Yes.
Threshold - Maximum increase in registered Analog Access gateways	Specify the maximum increase in registered Analog Access gateways that can occur before an event is raised. The default is 10%.
Event severity when increase in registered Analog Access gateways exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in registered Analog Access gateways exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for increase in registered Analog Access gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the increase in registered Analog Access gateways during the monitoring period.
Monitor Decrease in Registered Analog Access Gateways	
Event Notification	
Raise event if decrease in registered Analog Access gateways exceeds threshold?	Select **Yes** to raise an event if the decrease in registered Analog Access gateways exceeds the threshold you set. The default is Yes.
Threshold - Maximum decrease in registered Analog Access gateways	Specify the maximum decrease in registered Analog Access gateways that can occur before an event is raised. The default is 10%.
Event severity when decrease in registered Analog Access gateways exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of decrease in registered Analog Access gateways exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for decrease in registered Analog Access gateways?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in registered Analog Access gateways during the monitoring period.
Monitor Registered Other Station Devices	
Data Collection	
Collect data for registered other station devices?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of other station devices registered at each script iteration.

Parameter	How to Set It
Monitor Increase in Registered Other Station Devices	
Event Notification	
Raise event if increase in registered other station devices exceeds threshold?	Select **Yes** to raise an event if the increase in registered other station devices exceeds the threshold you set. The default is Yes.
Threshold - Maximum increase in registered other station devices	Specify the maximum increase in registered other station devices that can occur before an event is raised. The default is 10%.
Event severity when increase in registered other station devices exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in registered other station devices exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for increase in registered other station devices?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of increase in registered other station devices during the monitoring period.
Monitor Decrease in Registered Other Station Devices	
Event Notification	
Raise event if decrease in registered other station devices exceeds threshold?	Select **Yes** to raise an event if the decrease in registered other station devices exceeds the threshold you set. The default is Yes.
Threshold - Maximum decrease in registered other station devices	Specify the maximum decrease in registered other station devices that can occur before an event is raised. The default is 10%.
Event severity when decrease in registered other station devices exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of decrease in registered other station devices exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for decrease in registered other station devices?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of decrease in registered other station devices during the monitoring period.

CCM_ResourceAvailability

Use this Knowledge Script to monitor the number of times Communications Manager requests a resource that is unavailable. This script monitors the following resources:

- Annunciators
- Hardware, software, and video conference bridges
- Locations
- Media Termination Points (MTPs)
- Music-on-Hold (MOH)
- Transcoders

This script raises an event if an availability threshold is exceeded. In addition, this script generates data streams for instances of unavailability for each monitored resource.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 1172.

Resource Object

CiscoCM_CallProcessor

Default Schedule

By default, this script runs every 15 minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CCM_ResourceAvailability job. The default is 5.
Monitor Unavailable Annunciator Resources	
Event Notification	
Raise event if number of times annunciator resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times annunciator resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times annunciator resources were unavailable	Specify the maximum number of times an annunciator resource can be unavailable before an event is raised. The default is 0 times

Parameter	How to Set It
Event severity when number of times annunciator resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times an annunciator resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times annunciator resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times annunciator resources were unavailable during the monitoring period.
Monitor Unavailable Hardware Conference Bridge Resources	
Event Notification	
Raise event if number of times hardware conference bridge resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times hardware conference bridge resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times hardware conference bridge resources ere unavailable	Specify the maximum number of times a hardware conference bridge resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times hardware conference bridge resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times a hardware conference bridge resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times hardware conference bridge resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times hardware conference bridge resources were unavailable during the monitoring period.
Monitor Unavailable Software Conference Bridge Resources	
Event Notification	
Raise event if number of times software conference bridge resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times software conference bridge resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times software conference bridge resources were unavailable	Specify the maximum number of times a software conference bridge resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times software conference bridge resource were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times a software conference bridge resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for number of times software conference bridge resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times software conference bridge resources were unavailable during the monitoring period.
Monitor Unavailable Video Conference Bridge Resources	
Event Notification	
Raise event if number of times video conference bridge resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times video conference bridge resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times video conference bridge resources were unavailable	Specify the maximum number of times a video conference bridge resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times video conference bridge resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times a video conference bridge resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times video conference bridge resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times video conference bridge resources were unavailable during the monitoring period.
Monitor Unavailable Location Resources	
Event Notification	
Raise event if number of times location resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number times location resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times location resources were unavailable	Specify the maximum number of times a location resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times location resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times a location resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times location resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times location resources were unavailable during the monitoring period.
Monitor Unavailable Media Termination Point Resources	
Event Notification	
Raise event if number of times Media Termination Point resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times MTP resources were unavailable exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum number of times Media Termination Point resources were unavailable	Specify the maximum number of times an MTP resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times Media Termination Point resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times an MTP resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times Media Termination Point resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times MTP resources were unavailable during the monitoring period.
Monitor Unavailable Music-on-Hold Resources	
Event Notification	
Raise event if number of times Music-on-Hold resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times MOH resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times Music-on-Hold resources were unavailable	Specify the maximum number of times an MOH resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times Music-on-Hold resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times an MOH resource was unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times Music-on-Hold resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times MOH resources were unavailable during the monitoring period.
Monitor Unavailable Transcoder Resources	
Event Notification	
Raise event if number of times transcoder resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times transcoder resources were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times transcoder resources were unavailable	Specify the maximum number of times a transcoder resource can be unavailable before an event is raised. The default is 0 times.
Event severity when number of times transcoder resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times a transcoder resource was unavailable exceeds the threshold you set. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for number of times transcoder resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times transcoder resources were unavailable during the monitoring period.

CCM_SystemPerformance

Use this Knowledge Script to monitor call throttling and signal processing queues for a Communications Manager. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following metrics:

- Low, normal, and high priority signals that are processed and in queue
- Calls rejected due to throttling
- Throttled SCCP (Skinny Client Control Protocol) devices
- Number of times the Communications Manager went into a throttling state
- Average amount of expected delay

Throttling refers to an internal process within Communications Manager that prevents it from being inundated with heavy call traffic.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 1172.

Resource Object

CiscoCM_CallProcessor

Default Schedule

By default, this script runs every five minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CCM_SystemPerformance job. The default is 5.
Event Notification	
Raise event if call-throttling state entered?	Select **Yes** to raise an event if Communications Manager enters a call-throttling state. The default is Yes.
Event severity when call-throttling state entered	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Communications Manager enters a call-throttling state. The default is 10.
Raise event if severe call-throttling state entered?	Select **Yes** to raise an event if Communications Manager enters a severe call-throttling state. The default is Yes.
Event severity when severe call-throttling state entered	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Communications Manager enters a severe call-throttling state. The default is 5.

Parameter	How to Set It
Monitor High Priority Signals in Queue	
Event Notification	
Raise event if high priority signals in queue exceed threshold?	Select **Yes** to raise an event if the number of high-priority signals in queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum high priority signals in queue	Specify the maximum number of high-priority signals that must be in queue before an event is raised. The default is 25 signals.
Event severity when high priority signals in queue exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of high-priority signals in queue exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for high priority signals in queue?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of high-priority signals in queue at each script iteration.
Monitor High Priority Signals Processed	
Data Collection	
Collect data for high priority signals processed?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of high-priority signals that were recently processed at each script iteration.
Monitor Normal Priority Signals in Queue	
Event Notification	
Raise event if normal priority signals in queue exceed threshold?	Select **Yes** to raise an event if the number of normal priority signals in queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum normal priority signals in queue	Specify the maximum number of normal-priority signals that must be in queue before an event is raised. The default is 50 signals.
Event severity when normal priority signals in queue exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of normal-priority signals in queue exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for normal priority signals?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of normal-priority signals in queue at each script iteration.
Monitor Normal Priority Signals Processed	
Data Collection	
Collect data for normal priority signals processed?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of normal-priority signals that were recently processed at each script iteration.
Monitor Low Priority Signals in Queue	
Event Notification	
Raise event if low priority signals in queue exceed threshold?	Select **Yes** to raise an event if the number of low-priority signals in queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum low priority signals in queue	Specify the maximum number of low-priority signals that must be in queue before an event is raised. The default is 100 signals.

Parameter	How to Set It
Event severity when low priority signals in queue exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of low-priority signals in queue exceeds the threshold you set. The default is 10.
Data Collection	
Collect data for low priority signals in queue?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of low-priority signals in queue at each script iteration.
Monitor Low Priority Signals Processed	
Data Collection	
Collect data for low priority signals processed?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of low-priority signals that were recently processed at each script iteration.
Monitor Rejected Calls	
Event Notification	
Raise event if rejected calls exceed threshold?	Select **Yes** to raise an event if the number of rejected calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum rejected calls	Specify the maximum number of calls that must be rejected before an event is raised. The default is 0 calls.
Event severity when rejected calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of rejected calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for rejected calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls rejected during the monitoring period.
Monitor Throttled SCCP Devices	
Event Notification	
Raise event if throttled SCCP devices exceed threshold?	Select **Yes** to raise an event if the number of throttled SCCP devices exceeds the threshold you set. The default is Yes.
Threshold - Maximum throttled SCCP devices	Specify the maximum number of SCCP devices that must be throttled before an event is raised. The default is 0 devices.
Event severity when throttled SCCP devices exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of throttled SCCP devices exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for throttled SCCP devices?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of SCCP devices throttled during the monitoring period.
Monitor Call-Throttling	
Event Notification	
Raise event if number of times in call-throttling mode exceeds threshold?	Select **Yes** to raise an event if the number of times Communications Manager entered a call-throttling state exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times in call-throttling mode	Specify the maximum number of times Communications Manager must enter a call-throttling state before an event is raised. The default is 0 times.

Parameter	How to Set It
Event severity when number of times in call-throttling mode exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times Communications Manager entered a call-throttling state exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times in call-throttling mode?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times Communications Manager entered a call-throttling state during the monitoring period.
Monitor Average Expected Delay	
Event Notification	
Raise event if average expected delay exceeds threshold?	Select **Yes** to raise an event if the average amount of time it takes Communications Manager to handle incoming messages exceeds the threshold. The default is Yes.
Threshold - Maximum average expected delay	Specify the maximum amount of average delay Communications Manager can expect before an event is raised. The default is 2 seconds.
Event severity when average expected delay exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average amount of expected delay exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for average expected delay?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average amount of expected delay. The default is unselected.

CDR_CallFailures

Use this Knowledge Script to monitor call detail records (CDRs) retrieved from the primary Communications Manager for calls that ended with an abnormal termination code.

This script raises an event if the number of failed calls exceeds the threshold you set. In addition, this script generates a data stream for the number of failed calls.

The purpose of this script is threefold:

- **Monitoring**. In monitoring mode, this script checks the CDR tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in the CDR table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the CDR tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter.

  To run this script in troubleshooting mode, select **Run once** on the Schedule tab.
- **Diagnosing**. In diagnostic mode, this script works in conjunction with NetIQ Vivinet Diagnostics to diagnose VoIP quality problems detected monitoring. If the *Maximum number of failed calls* threshold is exceeded, then, by default, this script launches Action_DiagnoseVoIPQuality, a Knowledge Script that in turn launches Vivinet Diagnostics to generate a diagnosis of the problem.

  To turn off diagnostic mode, click the Actions tab, select **Action_DiagnoseVoIPQuality**, and click **Delete**. Turning diagnostic mode off or on does not affect the events raised by this script.

Prerequisites

- Run the SetupSupplementalDB Knowledge Script to create the Cisco CM supplemental database that will house the call detail records.
- Run the CDR_RetrieveCallRecords and CDR_RetrieveConfigData Knowledge Script to populate the database.

For more information, see "Understanding the Cisco CM Supplemental Database" on page 1144.

Resource Object

CiscoCM_CDRMgmt

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CallFailures job. The default is 5.

Parameter	How to Set It
Include call details?	Select **Yes** to include call details in the events raised by this script. Leave this parameter unchecked to suppress call details. If you select **Yes**, an event includes the following details: • Originating Device Name • Originating IP Address • Calling Party Number • Originating Media Cap - Payload Capacity • Destination Device Name • Destination IP Address • Original Called Party Number • Final Called Party Number • Originating Cause • Destination Cause
Raise event if no records found?	Select **Yes** to raise an event if there are no CDRs to monitor. Note that we do not mean there are no CDRs with abnormal termination codes, but that there are no CDRs at all. The default is unselected.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no CDRs were found. The default is 25.
Query Filters No matter how many calls AppManager may find that match the filters you select, an event displays only the first 50 calls.	
Ignore unknown cause codes?	Select **Yes** if you want to ignore CDRs that have cause codes of "Unknown." The default is unselected.
Exclude these failure codes	Type a list of termination codes (separated by commas) that are not to be considered failures. See Termination Codes for a list of available codes. **Note** Codes 0, 16, 31, and 127 are automatically excluded. They are normal termination codes. However, these codes may appear in events if the other side of the call has a failure code that has not been excluded.
Minimum duration	Set this parameter to filter out records whose call duration is less than the specified value. Accept the default of 0 to ignore the filter for minimum call duration.
Maximum duration	Set this parameter to filter out records whose call duration is less than or equal to the specified value. Accept the default of 0 to ignore the filter for maximum call duration.
Calling directory number	Specify the number of the calling directory you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any calling directory number.
Directory number connector	Set this parameter ONLY if you specify both a **Calling directory number** and a **Called directory number**. Your selection indicates how the script will connect the two parameters: AND or OR. The default is AND.
Called directory number	Specify the number of the called directory you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any called directory number.
Originating device name	Set this parameter to query for those calls whose originating device name matches the specified value. Wildcard characters are acceptable. Leave this parameter blank to search for any originating device name.
Device name connector	Set this parameter ONLY if you specify both an **Originating device name** and a **Destination device name**. Your selection indicates how the script will connect the two parameters: AND or OR. The default is AND.

Parameter	How to Set It
Destination device name	Set this parameter to query for those calls whose destination device name matches the specified value. Wildcard characters are acceptable. Leave this parameter blank to search for any destination device name.
Troubleshooting	
Select call disconnect time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **Note** This parameter is valid only when you select **Run once** on the **Schedule** tab.
Monitor Failed Calls	
Event Notification	
Raise event if number of failed calls exceeds threshold?	Select **Yes** to raise an event if the number of calls that failed with an abnormal termination code exceeds the threshold. The default is Yes.
Threshold - Maximum number of failed calls	Specify the maximum number of calls that can fail before an event is raised. The default is 0 calls.
Event severity when number of failed calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of failed calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of failed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that failed with an abnormal termination code during the monitoring period.

Termination Codes

Use this list of termination codes (also known as call release cause codes) to complete the *Exclude these failure codes* parameter.

Termination Code	Description	Explanation
0	No error	No error.
1	Unallocated (unassigned) number	Indicates the called party cannot be reached because, although the called party number is in a valid format, it is not currently allocated (assigned).
2	No route to specified transit network (national use)	Indicates one of the following: • The equipment sending this code has received a request to route the call through a transit network that it does not recognize. The equipment does not recognize the transit network either because the transit network does not exist or because the transit network exists but does not serve the equipment that is sending the code. • The prefix 0 is invalid for the entered number.
3	No route to destination	Indicates one of the following: • The called party cannot be reached because the network through which the call has been routed does not service the desired destination. This cause is supported on a network-dependent basis. • A 1 was dialed when not required. Redial without the 1.

Termination Code	Description	Explanation
4	Send special information tone	Indicates one of the following: • The prefix 1 is not required for this number. • The called party cannot be reached for reasons of a long-term nature. The special information tone should be returned to the calling party.
5	Misdialed trunk prefix (national use)	Indicates the erroneous inclusion of a trunk prefix in the called party number.
6	Channel unacceptable	Indicates a called user cannot negotiate for a B-channel other than that specified in the SETUP message.
7	Call awarded and being delivered in an established channel	Indicates the user has been awarded the incoming call and the call is being connected to a channel (such as packet mode or X.25 virtual calls) already established to that user for similar calls.
8	Preemption	Indicates a call has been preempted.
9	Preemption - circuit reserved for reuse	Indicates a call has been preempted because the circuit is reserved for reuse.
16	Normal call clearing	Indicates normal call clearing has occurred.
17	User busy	Indicates the called party is unable to accept another call because the user busy condition has been encountered. Code 17 may be generated by the called user or by the network. In the case of user-determined user busy, it is noted that the user equipment is compatible with the call.
18	No user responding	Indicates a called party does not respond to a call establishment message with an alerting or connect indication within the allotted prescribed period of time (before timer T303 or T310 has expired).
19	No answer from user (user alerted)	Indicates the called user has provided an alerting indication, but not a connect indication within a prescribed period of time (before timer T301 has expired).
20	Subscriber absent	Indicates one of the following:· • A mobile station has logged off. • Radio contact is not obtained with a mobile station. • A personal telecommunications user is temporarily not addressable at any user-network interface.
21	Call rejected	Indicates one of the following: • The equipment sending this cause does not wish to accept the call, although it could have accepted the call because it is neither busy nor incompatible. • May be generated by the network, indicating the call was cleared due to a supplementary service constraint.
22	Number changed	Indicates the called party number indicated by the calling party is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this cause, then cause #1 shall be used.
26	Non-selected user clearing	Indicates the user has not been awarded the incoming call.

Termination Code	Description	Explanation
27	Destination out of order	Indicates the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" indicates a signal message was unable to be delivered to the remote party, as in the following examples: • Physical layer or data link layer failure at the remote party • User equipment off-line
28	Invalid number format (address incomplete)	Indicates one of the following: • The called party cannot be reached because the called party number is not in a valid format or is not complete. • The user should be returned a Special Intercept Announcement.
29	Facility rejected	Indicates one of the following: • The network cannot provide the requested facility. • A user in a special business group, such as a Centrex, dialed an undefined code.
30	Response to STATUS ENQUIRY	Indicates one of the following: • This cause is included in the Status Message when the reason for sending the Status Message was the previous receipt of a Status Enquiry message. • A user from outside a basic business group, such as a Centrex, has violated an access restriction feature.
31	Normal, unspecified	Used to report a normal event only when no other cause in the normal class applies.
34	No circuit/channel available	Indicates no appropriate circuit or channel is available to handle the call.
38	Network out of order	Indicates the network is not functioning correctly and the condition is likely to last a relatively long time. Immediately re-attempting the call is not likely to be successful.
39	Permanent frame mode connection out of service	Indicates a permanent connection was terminated, probably due to equipment failure.
40	Permanent frame mode connection operational	Indicates a permanent connection is operational again. The connection was previously terminated, probably due to equipment failure.
41	Temporary failure	Indicates the network is not functioning correctly and the condition is not likely to last a long time. The user may wish to attempt another call almost immediately. May also indicate a data link layer malfunction locally or at the remote network interface, or a call was cleared due to protocol error(s) at the remote network interface.
42	Switching equipment congestion	Indicates the switching equipment generating this cause is experiencing a period of high traffic.
43	Access information discarded	Indicates the network is unable to deliver user information (such as user-to-user information, low-level compatibility, or sub-address) to the remote users as requested.
44	Requested circuit/channel not available	Indicates the other side of the interface cannot provide the circuit or channel indicated by the requesting entity.

Termination Code	Description	Explanation
46	Precedence call blocked	Indicates the remote device that was called is busy.
47	Resource unavailable, unspecified	Indicates one of the following: • No other cause in the resource unavailable class applies. • The original destination is unavailable. Invoke redirection to a new destination.
49	Quality of Service not available	Indicates the network cannot provide the requested Quality of Service. May be a subscription problem.
50	Requested facility not subscribed	Indicates this facility is unavailable because the user has not subscribed to it.
53	Service operation violated	Indicates the user has violated the service operation.
54	Incoming calls barred	Indicates the user will not accept the call delivered in the SETUP message.
55	Incoming calls barred within Closed User Group (CUG)	Indicates the network does not allow the user to receive calls.
57	Bearer capability not authorized	Indicates the user has requested a bearer capability implemented by the equipment that generated this cause. However, the user is not authorized to use it. This common problem is caused by incorrect Telco provisioning of the line at the time of installation.
58	Bearer capability not presently available	Indicates the user has requested a bearer capability implemented by the equipment that generated this cause. However, bearer capability is unavailable at the present time. This problem may be due to a temporary network problem or a subscription problem.
62	Inconsistency in designated outgoing access information and subscriber class	Indicates an inconsistency in the designated outgoing access information and subscriber class.
63	Service or option not available, unspecified	Indicates a service or option is not available. Used only when no other cause in this class applies.
65	Bearer capability not implemented	Indicates the equipment sending this cause does not support the requested bearer capability.
66	Channel type not implemented	Indicates the called party has reached an unsupported channel type.
69	Requested facility not implemented	Indicates the network (or node) does not support the requested bearer capability and therefore cannot be accessed at this time.
70	Only restricted digital information bearer capability available (national use)	Indicates the calling party has requested an unrestricted bearer service. However, the equipment sending this cause supports only the restricted version of the requested bearer capability.
79	Service or option not implemented, unspecified	Indicates a service or option was not implemented. Used only when no other cause in this class applies.
81	Invalid call reference value	Indicates the equipment sending this cause has received a message with a call reference not currently in use on the user-network interface. This value applies only if the call reference value is 1 or 2 octets long and is not the global call reference.
82	Identified channel does not exist	Indicates the equipment sending this cause has received a request to use a channel not active on the interface for a call.

Termination Code	Description	Explanation
83	A suspended call exists, but this call identity does not	Indicates suspended call exists but the call's identity does not.
84	Call identity in use	Indicates a call identity is in use.
85	No call suspended.	Indicates no call is suspended.
86	Call having the requested call identity has been cleared	Indicates the call having the requested call identity has cleared.
87	User not member of Closed User Group (CUG)	Indicates the call was not completed, probably due to one of the following reasons: • The dialed number is incorrect • The user is not authorized to use (or has not subscribed to) the requested service • User is using a service the remote device is not authorized to use
88	Incompatible destination	Indicates the equipment sending this cause has received a request to establish a call that has low layer compatibility, high layer compatibility, or other compatibility attributes (such as data rate or DN subaddress), which cannot be accommodated. This call can be returned by a switch to a CPE when trying to route a call to an incompatible facility, or one without a data rate.
90	Destination number missing and DC not subscribed	Indicates the call was not completed, probably due to one of the following reasons: • The dialed number is incorrect • The user is not authorized to use (or has not subscribed to) the requested service • User is using a service the remote device is not authorized to use
91	Invalid transit network selection (national use)	Indicates an invalid transit network selection has been requested.
95	Invalid message, unspecified	Indicates the entity sending this cause has received an invalid message. Used when no other cause in this class applies.
96	Mandatory information element is missing	Indicates the equipment sending this cause has received a message missing an information element that must be present in the message before the message can be processed.
97	Message type non-existent or not implemented	Indicates one of the following: • The equipment sending this cause has received a message type it does not recognize. Either the message is not defined, or it is defined and not implemented by the equipment sending this cause. • A problem with the remote configuration or with the local D-channel.
98	Message not compatible with the call state, or the message type is non-existent or not implemented	Indicates one of the following: • Message received is not compatible with the call state • Message type is non-existent or not implemented

Termination Code	Description	Explanation
99	An information element or parameter non-existent or not implemented	Indicates the equipment sending this cause has received a message that includes information elements not recognized because either the information element identifier is not defined, or it is defined but not implemented by the equipment sending the cause. However, the information element is not required for the equipment sending the cause to process the message.
100	Invalid information element contents	Indicates the equipment sending this cause has received an information element it has implemented. However, one or more fields of the information elements are coded in such a way (such as truncated, invalid extension bit, invalid field values) that the information element has not been implemented by the equipment sending this cause.
101	The message not compatible with the call state	Indicates one of the following: • The equipment sending this cause has received a message procedures indicate is not a permissible message to receive at this time. • The switch sending this cause is clearing the call because a threshold has been exceeded for multiple protocol errors during an active call.
102	Call terminated when timer expired; a recovery routine executed to recover from the error	Indicates a procedure has been initiated by the expiration of a timer in associated with error-handling procedures.
103	Parameter non-existent or not implemented - passed on (national use)	Indicates the equipment sending this cause has received a message that includes parameters not recognized because the parameters are defined but not implemented by the equipment sending the cause. The parameters were ignored. In addition, if the equipment sending this cause is an intermediate point, then this cause indicates the parameters were passed on unchanged.
110	Message with unrecognized parameter discarded	Indicates the equipment sending this cause has discarded a received message that includes a parameter that is not recognized.
111	Protocol error, unspecified	Reports a protocol error event only when no other cause in this class applies. This cause may be displayed if the user failed to dial a 9 or an 8 for an outside line. In addition, this cause may be returned in the event of certain types of restrictions as to number of calls.
122	Precedence level exceeded	Indicates users attempted to make a call with a higher level of precedence than the highest precedence level authorized for their line.
123	Device not preemptable	Indicates one of the following: • The dialed number is non preemptable. That is, the dialed number registers as busy and has no call waiting, no call forwarding, and no alternate party designations. • The dialed number has a higher precedence level (or priority) than the dialing number and cannot be preempted.
125	Out of bandwidth	Indicates not enough bandwidth was found to connect a call to the destination location.

Termination Code	Description	Explanation
127	Interworking, unspecified	Indicates an interworking call (usually a call to SW56 service) has ended. May also be seen in the event of a non-specific rejection by a long distance carrier.
129	Precedence out of bandwidth	Indicates not enough bandwidth was found to connect a precedence call to the destination location.
162144 0x40000	Conference full	A Cisco-specific code. Indicates a conference is at full capacity and can accept no new callers.
393216 0x60000	Call split	A Cisco-specific code. Indicates a call was terminated during a transfer operation because it was split off and terminated (not part of the final transferred call). This code can help determine which calls were terminated as part of a feature operation.
458752 0x70000	Drop any party/drop last party	A Cisco-specific code. Indicates a call was dropped from a conference by the new feature "drop any party/drop last party."

CDR_CallQuality

Use this Knowledge Script to monitor call detail records (CDRs) and call management records (CMRs) retrieved from the primary Communications Manager for jitter, latency, packet loss, and MOS (Mean Opinion Score).

This script raises an event if a monitored value exceeds or falls below a threshold. In addition, this script generates data streams for average and minimum MOS, and maximum jitter, latency, and packet loss.

The purpose of this script is threefold:

- **Monitoring**. In monitoring mode, this script checks the CDR tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in the CDR table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the CDR tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter.

  To run this script in troubleshooting mode, select **Run once** on the Schedule tab.
- **Diagnosing**. In diagnostic mode, this script works in conjunction with NetIQ Vivinet Diagnostics to diagnose VoIP quality problems detected during monitoring. If a call quality threshold is exceeded, then, by default, this script launches Action_DiagnoseVoIPQuality, a Knowledge Script that in turn launches Vivinet Diagnostics to generate a diagnosis of the problem.

  To turn off diagnostic mode, click on the Actions tab, select **Action_DiagnoseVoIPQuality**, and click **Delete**. Turning diagnostic mode off or on does not affect the events raised by this script.

Prerequisites

- Run the SetupSupplementalDB Knowledge Script to create the Cisco CM supplemental database that will house the call detail records.
- Run the CDR_RetrieveCallRecords and CDR_RetrieveConfigData Knowledge Script to populate the database.

For more information, see "Understanding the Cisco CM Supplemental Database" on page 1144.

Resource Object

CiscoCM_CDRMgmt

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	

Parameter	How to Set It
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CDR_CallQuality job. The default is 5.
Include call details?	Select **Yes** to include call details in the events raised by this script. Leave this parameter unchecked to suppress call details. If you select **Yes**, an event includes the following details: • Average and minimum MOS • Jitter • Latency • Lost Packets (%) • Originating and Destination Devices • Calling and Called Numbers • Origination and Disconnect Times • Duration (seconds) • Calling and Called Number Partitions
Raise event if no records found?	Select **Yes** to raise an event if there are no CDRs to monitor. Note that we do not mean there are no CDRs with call quality data, but that there are no CDRs at all. The default is unselected.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no CDRs were found. The default is 25.
Query Filters • No matter how many calls AppManager may find that match the filters you select, an event displays only the first 50 calls. • Regardless of the filters you select (or if you select no filters at all), an event displays call data in two tables labeled Inbound and Outbound. The Inbound table contains details of calls coming into the Originating Device (according to the CMR table). The Outbound table contains details of calls going out from the Originating Device (according to the CMR table).	
Minimum duration	Set this parameter to filter out records whose call duration is less than the specified value. Accept the default of 0 to ignore the filter for minimum duration.
Maximum duration	Set this parameter to filter out records whose call duration is more than or equal to the specified value. Accept the default of 0 to ignore the filter for maximum duration.
Directory number	Set this parameter to query for those calls whose directory number matches the specified value. Wildcard characters are acceptable. Leave this parameter blank to search for any directory number.
Device name	Set this parameter to query for those calls whose device name matches the specified value. Wildcard characters are acceptable. Leave this parameter blank to search for any device name.
Troubleshooting	
Select call disconnect time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **Note** This parameter is valid only when you select **Run once** on the **Schedule** tab.
Monitor Average Acceptable Listening MOS	
Event Notification	
Raise event if average MOS falls below threshold?	Select **Yes** to raise an event if the average MOS value falls below the threshold. The default is Yes.
Threshold - Average MOS	Specify the lowest average MOS value that must occur to prevent an event from being raised. The default is 3.60.

Parameter	How to Set It
Event severity when average MOS falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average MOS value falls below the threshold. The default is 5.
Data Collection	
Collect data for average MOS?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average MOS value during the monitoring period.
Monitor Minimum Acceptable Listening MOS	
Event Notification	
Raise event if minimum MOS falls below threshold?	Select **Yes** to raise an event if the minimum MOS value falls below the threshold. The default is Yes.
Threshold - Minimum MOS	Specify the lowest MOS value that must occur to prevent an event from being raised. The default is 3.60.
Event severity when minimum MOS falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the minimum MOS value falls below the threshold. The default is 5.
Data Collection	
Collect data for minimum MOS?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the minimum MOS value during the monitoring period.
Monitor Jitter	
Event Notification	
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if the jitter value exceeds the threshold. The default is Yes.
Threshold - Maximum jitter	Specify the highest jitter value that can occur before an event is raised. The default is 60 milliseconds.
Event severity when jitter exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the jitter value exceeds the threshold. The default is 15.
Data Collection	
Collect data for jitter?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of jitter that occurred during the monitoring period.
Monitor Latency	
Event Notification	
Raise event if latency exceeds threshold?	Select **Yes** to raise an event if the latency value exceeds the threshold. The default is Yes.
Threshold - Maximum latency	Specify the highest amount of latency that can occur before an event is raised. The default is 400 milliseconds.
Event severity when latency exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the latency value exceeds the threshold. The default is 15.
Data Collection	
Collect data for latency?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of latency that occurred during the monitoring period.
Monitor Packet Loss	
Event Notification	
Raise event if packet loss exceeds threshold?	Select **Yes** to raise an event if the packet loss value exceeds the threshold. The default is Yes.

Parameter	How to Set It
Threshold - Maximum packet loss	Specify the highest amount of packet loss that can occur before an event is raised. The default is 1%.
Event severity when packet loss exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the packet loss value exceeds the threshold. The default is 15.
Data Collection	
Collect data for packet loss?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of packet loss that occurred during the monitoring period.

CDR_Query

Use this Knowledge Script to search for call detail records (CDRs) retrieved from the primary Communications Manager and stored in the local SQL database. The search is based on query filters you select. This script raises an event if no CDRs are found or if the number of CDRs found exceeds the threshold you set. In addition, this script generates a data stream for the number of records found.

The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the CDR tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in the CDR table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the CDR tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter.

  To run this script in troubleshooting mode, select **Run once** on the Schedule tab.

Resource Object

CiscoCM_CDRMgmt

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CDR_Query job. The default is 5.
Raise event if no records found?	Select **Yes** to raise an event if there are no CDRs to monitor. Note that we do not mean there are no CDRs with call quality data, but that there are no CDRs at all. The default is unselected.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no CDRs were found. The default is 25.
Query Filters No matter how many calls AppManager may find that match the filters you select, an event displays only the first 50 calls.	
Minimum duration	Set this parameter to filter out records whose call duration is less than the specified value. Accept the default of 0 to ignore the filter for minimum call duration.
Maximum duration	Set this parameter to filter out records whose call duration is less than or equal to the specified value. Accept the default of 0 to ignore the filter for maximum call duration.

Parameter	How to Set It
Calling directory number	Specify the number of the calling directory you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any calling directory number.
Directory number connector	Set this parameter ONLY if you specify both a **Calling directory number** and a **Called directory number**. Your selection indicates how the script will connect the two parameters: AND or OR. The default is AND.
Called directory number	Specify the number of the called directory you want to find in the CDRs. Wildcard characters are acceptable. Leave this parameter blank to search for any called directory number.
Originating device name	Set this parameter to query for those calls whose originating device name matches the specified value. Wildcard characters are acceptable. Leave this parameter blank to search for any originating device name.
Device name connector	Set this parameter ONLY if you specify both an **Originating device name** and a **Destination device name**. Your selection indicates how the script will connect the two parameters: AND or OR. The default is AND.
Destination device name	Set this parameter to query for those calls whose destination device name matches the specified value. Wildcard characters are acceptable. Leave this parameter blank to search for any destination device name.
Troubleshooting	
Select call disconnect time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **Note** This parameter is valid only when you select **Run once** on the Schedule tab.
Monitor Records Found	
Event Notification	
Raise event if number of records exceeds threshold?	Select **Yes** to raise an event if the number of CDRs found exceeds the threshold. The default is Yes.
Threshold - Maximum number of records	Specify the maximum number of CDRs that can be found before an event is raised. The default is 0 CDRs.
Event severity when number of records exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of CDRs found exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of records?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of CDRs found during the monitoring period.

CDR_RetrieveCallRecords

The primary Communications Manager sends call detail records (CDRs) to a folder you specified on the proxy agent computer. Use this script to retrieve the CDRs from the folder and insert them into the Cisco CM supplemental database. This script will archive the records, if indicated.

Prerequisite

Run the SetupSupplementalDB Knowledge Script to create the supplemental database. For more information, see "Understanding the Cisco CM Supplemental Database" on page 1144.

Resource Object

CiscoCM_CDRMgmt

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CDR_RetrieveCallRecords job. The default is 5.
Archive call detail records after processing?	Select **Yes** to copy CDRs to an archive folder after processing. If you leave this parameter unchecked, CDRs are deleted after processing.
Archive folder	Specify the full path to a location on the agent computer in which to create the archive folder.

CDR_RetrieveConfigData

Use this Knowledge Script to retrieve Communications Manager configuration data from the primary Communications Manager and store it in the Cisco CM supplemental database.

Prerequisite

Run the SetupSupplementalDB Knowledge Script to create the supplemental database that will house the configuration data. For more information, see "Understanding the Cisco CM Supplemental Database" on page 1144.

Resource Object

CiscoCM_CDRMgmt

Default Schedule

By default, this script runs once a day, at 3 A.M, so as to perform its possibly CPU-intensive function at a time when the Communications Manager is least busy.

However, because the PhoneDeregistrations script uses the configuration data this script retrieves, you may want to set this script to "Run Once" so the configuration data is retrieved immediately. When the "Run Once" job is complete, you can then run this script using the default schedule of once daily.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CDR_RetrieveConfigData job. The default is 5.
Raise event if data collection succeeds?	Select **Yes** to raise an event if the data-collection process succeeds. The default is unselected.
Event severity when data collection succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data collection succeeds. The default is 25.

CFB_Hardware_Device

Use this Knowledge Script to monitor the resource usage of a registered hardware conference bridge device.

- Active conferences
- Completed conferences
- Resource usage
- Active resources
- Unavailable resources

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for active and completed conferences, active resources, and resource usage (%).

Resource Object

CiscoCM_HW_CFBObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CFB_Hardware_Device job. The default is 5.
Monitor Active Conferences	
Event Notification	
Raise event if active conferences exceed threshold?	Select **Yes** to raise an event if the number of active hardware conferences exceeds the threshold you set. The default is Yes.
Threshold - Maximum active conferences	Specify the maximum number of hardware conferences that must be active before an event is raised. The default is 250 conferences.
Event severity when active conferences exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active hardware conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for active conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of hardware conferences active during the monitoring period.
Monitor Completed Conferences	
Data Collection	

Parameter	How to Set It
Collect data for completed conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of hardware conferences completed during the monitoring period.
Monitor Resource Usage	
Event Notification	
Raise event if resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of hardware conference usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum resource usage	Specify the maximum percentage of hardware conference usage that must be detected before an event is raised. The default is 80%.
Event severity when resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of hardware conference usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of hardware conference usage at each script iteration.
Monitor Active Resources	
Data Collection	
Collect data for active resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of hardware conferences active at each script iteration.
Monitor Unavailable Resources	
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times hardware conferences were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times hardware conferences must be unavailable before an event is raised. The default is 0 instances.
Event severity when number of times resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times hardware conferences were unavailable exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times hardware conferences were unavailable during the monitoring period.

CFB_Software_Device

Use this Knowledge Script to monitor the resource usage of a registered software conference bridge device.

- Active conferences
- Completed conferences
- Resource usage
- Active resources
- Unavailable resources

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for active and completed conferences, active resources, and resource usage (%).

Resource Object

CiscoCM_SW_CFBObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CFB_Software_Device job. The default is 5.
Monitor Active Conferences	
Event Notification	
Raise event if active conferences exceed threshold?	Select **Yes** to raise an event if the number of active software conferences exceeds the threshold you set. The default is Yes.
Threshold - Maximum active conferences	Specify the maximum number of software conferences that must be active before an event is raised. The default is 250 conferences.
Event severity when active conferences exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active software conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for active conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of software conferences active during the monitoring period.
Monitor Completed Conferences	
Data Collection	

Parameter	How to Set It
Collect data for completed conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of software conferences completed during the monitoring period.
Monitor Resource Usage	
Event Notification	
Raise event if resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of software conference resource usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum resource usage	Specify the maximum percentage of software conference resource usage that must be detected before an event is raised. The default is 80%.
Event severity when resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of software conference resource usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of software conference resource usage at each script iteration.
Monitor Active Resources	
Data Collection	
Collect data for active resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of software conference resources active at each script iteration.
Monitor Unavailable Resources	
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times a software conference resource was unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times software conference resources must be unavailable before an event is raised. The default is 0 conferences.
Event severity when number of times resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times software conference resources were unavailable exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times software conference resources were unavailable.

CFB_Video_Device

Use this Knowledge Script to monitor the resource usage of a registered video conference bridge device.

- Active conferences
- Completed conferences
- Resource usage
- Active resources
- Unavailable resources

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for active and completed conferences, active resources, and resource usage (%).

Resource Object

CiscoCM_VideoCFBObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CFB_Video_Device job. The default is 5.
Monitor Active Conferences	
Event Notification	
Raise event if active conferences exceed threshold?	Select **Yes** to raise an event if the number of active video conferences exceeds the threshold you set. The default is Yes.
Threshold - Maximum active conferences	Specify the maximum number of video conferences that must be active before an event is raised. The default is 250 conferences.
Event severity when active conferences exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active video conferences exceeds the threshold. The default is 10.
Data Collection	
Collect data for active conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of video conferences active during the monitoring period.
Monitor Completed Conferences	
Data Collection	
Collect data for completed conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of video conferences completed during the monitoring period.

Parameter	How to Set It
Monitor Resource Usage	
Event Notification	
Raise event if resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of video conference usage exceeds the threshold you set. The default is Yes.
Threshold - Maximum resource usage	Specify the maximum percentage of video conference usage that must be detected before an event is raised. The default is 80%.
Event severity when resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of video conference usage exceeds the threshold. The default is 10.
Data Collection	
Collect data for resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of video conference usage at each script iteration.
Monitor Active Resources	
Data Collection	
Collect data for active resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of video conferences active at each script iteration.
Monitor Unavailable Resources	
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times video conferences were unavailable exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times video conferences must be unavailable before an event is raised. The default is 0 instances.
Event severity when number of times resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times video conferences were unavailable exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times video conferences were unavailable during the monitoring period.

CTIManager

Use this Knowledge Script to monitor the usage of the Communications Manager CTI Manager. CTI Manager allows applications to access the resources and functionality of all Communications Managers in the cluster.

This script raises an event if a value exceeds or falls below its threshold. In addition, this script generates data streams for the number of connected applications, open lines, open devices, and active Communications Manager links.

Resource Object

CiscoCM_CTIMgrService

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CTIManager job. The default is 5.
Monitor Connected Applications	
Event Notification	
Raise event if connected applications exceed threshold?	Select **Yes** to raise an event if the number of connected applications exceeds the threshold you set. The default is Yes.
Threshold - Maximum connected applications	Specify the maximum number of applications that must be connected before an event is raised. The default is 100 applications.
Event severity when connected applications exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of connected applications exceeds the threshold. The default is 15.
Data Collection	
Collect data for connected applications?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of applications connected at each script iteration.
Monitor Open Lines	
Event Notification	
Raise event if open lines exceed threshold?	Select **Yes** to raise an event if the number of open lines exceeds the threshold you set. The default is Yes.
Threshold - Maximum open lines	Specify the maximum number of lines that must be open before an event is raised. The default is 100 lines.
Event severity when open lines exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of open lines exceeds the threshold. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for open lines?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of lines open at each script iteration.
Monitor Open Devices	
Event Notification	
Raise event if open devices exceed threshold?	Select **Yes** to raise an event if the number of open devices exceeds the threshold you set. The default is Yes.
Threshold - Maximum open devices	Specify the maximum number of devices that must be open before an event is raised. The default is 100 devices.
Event severity when open devices exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of open devices exceeds the threshold. The default is 15.
Data Collection	
Collect data for open devices?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of devices open at each script iteration.
Monitor Active CallManager Links	
Event Notification	
Raise event if active CallManager links fall below threshold?	Select **Yes** to raise an event if the number of active Communications Manager links falls below the threshold you set. The default is Yes.
Threshold - Minimum active CallManager links	Specify the minimum number of Communications Manager links that must be active before an event is raised. The default is one link.
Event severity when active CallManager links fall below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active Communications Manager links falls below the threshold. The default is 15.
Data Collection	
Collect data for active CallManager links?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of Communications Manager links active at each script iteration.

ExtensionMobility

Use this Knowledge Script to monitor the Extension Mobility application. Extension Mobility allows users to temporarily access their Cisco IP phone configuration, such as line appearances, services, and speed dials, from other Cisco IP phones.

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the number of throttled requests, in-progress requests, login/logout requests, successful logins, successful logouts, and total requests.

Resource Object

CiscoCM_ExtMobility

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the ExtensionMobility job. The default is 5.
Monitor Login/Logout Requests	
Event Notification	
Raise event if login/logout requests exceed threshold?	Select **Yes** to raise an event if the number of requests to log in or log out exceeds the threshold you set. The default is Yes.
Threshold - Maximum login/ logout requests	Specify the maximum number of login and logout requests that must occur before an event is raised. The default is 100 requests.
Event severity when login/ logout requests exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of login and logout requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for login/logout requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of login and log out requests that occurred during the monitoring period.
Monitor Successful Logins	
Data Collection	
Collect data for successful logins?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of logins that were successful during the monitoring period.
Monitor Successful Logouts	
Data Collection	

Parameter	How to Set It
Collect data for successful logouts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of logouts that were successful during the monitoring period.
Monitor Requests in Progress	
Event Notification	
Raise event if requests in progress exceed threshold?	Select **Yes** to raise an event if the number of in-progress requests exceeds the threshold you set. The default is Yes.
Threshold - Maximum requests in progress	Specify the maximum number of requests that must be in progress before an event is raised. The default is 500 requests.
Event severity when requests in progress exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-progress requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for requests in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of requests in progress at each script iteration.
Monitor Throttled Requests	
Event Notification	
Raise event if throttled requests exceed threshold?	Select **Yes** to raise an event if the number of throttled requests exceeds the threshold you set. The default is Yes.
Threshold - Maximum throttled requests	Specify the maximum number of requests that must be throttled before an event is raised. The default is 10 requests.
Event severity when throttled requests exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of throttled requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for throttled requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of requests throttled during the monitoring period.
Monitor Total Requests	
Data Collection	
Collect data for total requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of all requests that occurred during the monitoring period.

GatekeeperActivity

Use this Knowledge Script to monitor the activity on a gatekeeper. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following monitored activities:

- Received admission confirm messages (ACFs)
- Attempted admission requests
- Retried acknowledgement messages (RASs)
- Failed video stream requests

Resource Object

CiscoCM_GatekeeperObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the GatekeeperActivity job. The default is 5.
Monitor Failed Video Stream Requests	
Event Notification	
Raise event if failed video stream requests exceed threshold?	Select **Yes** to raise an event if the number of failed video stream requests exceeds the threshold you set. The default is Yes.
Threshold - Maximum failed video stream requests	Specify the maximum number of video stream requests that must fail before an event is raised. The default is 0 requests.
Event severity when failed video stream requests exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of failed video stream requests exceeds the threshold. The default is 15.
Data Collection	
Collect data for failed video stream requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of video stream requests that failed during the monitoring period.
Monitor Retries	
Event Notification	
Raise event if retries exceed threshold?	Select **Yes** to raise an event if the number of RASs exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum retries	Specify the maximum number of acknowledgement messages that must be retried before an event is raised. The default is 50 messages.
Event severity when retries exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of RASs exceeds the threshold. The default is 15.
Data Collection	
Collect data for retries?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of acknowledgement messages that were retried during the monitoring period.
Monitor Admission Confirm Messages	
Data Collection	
Collect data for admission confirm messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of ACFs received during the monitoring period.
Monitor Admission Request Messages	
Data Collection	
Collect data for admission request messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of admission requests attempted during the monitoring period.

GeneralCounter

Use this Knowledge Script to monitor a user-specified Performance Monitor counter on a Communications Manager server. You can monitor both the current value of the counter as well as the delta value (current value minus the previous value). This script raises an event if the value of the monitored counter exceeds the threshold and if the counter you want to monitor is not accessible.

This script generates data streams for current and delta counter values.

Resource Object

CiscoCM_CMServer

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the GeneralCounter job.
Counter Specifications	
Name of the object to monitor	Type the name of the performance object you want to monitor. An object is any resource, program or service for which performance data can be collected. The default object name is System.
Name of the counter to monitor	Type the name of the performance counter you want to monitor. A counter represents the data associated with aspects of an object. The default counter name is `Total Threads`.
Name of the instance to monitor	Type the name of the performance instance you want to monitor. An instance distinguishes between multiple objects of the same type on a single computer. You can type multiple instance names, separated by commas. Not all counters or objects require or have an instance.
Raise event if counter/ instance not found?	Select **Yes** to raise an event if this script cannot find the counter or instance you specify. The default is Yes.
Event severity when counter/ instance not found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this script cannot find the counter or instance you specify. The default is 25.
Monitor Current Value	
Event Notification	
Raise event if current value exceeds threshold	Select **Yes** to raise an event if the current value of the counter exceeds the threshold you set. The default is Yes.
Threshold - Maximum current value	Specify the maximum current value the counter can attain before an event is raised. The default is 500.

Parameter	How to Set It
Event severity when current value exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the current value of the counter exceeds the threshold you set. The default is 10.
Data Collection	
Collect data for current value?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the current value of the counter at each script iteration.
Monitor Delta Value	
Event Notification	
Raise event if delta value exceeds threshold	Select **Yes** to raise an event if the delta value of the counter exceeds the threshold you set. The default is Yes. The delta value is the difference between the current value and the previous value.
Threshold - Maximum delta value	Specify the maximum delta value the counter can attain before an event is raised. The default is 100.
Event severity when delta value exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the delta value of the counter exceeds the threshold you set. The default is 10.
Data Collection	
Collect data for delta value?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the delta value of the counter as measured during the monitoring period.

H323_Gateway_CallActivity

Use this Knowledge Script to monitor completed, attempted, in-progress, and active calls on an H.323 gateway device. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for completed calls, attempted calls, in-progress calls, and active calls.

Resource Object

CiscoCM_H323GatewayObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the H323_Gateway_CallActivity job.
Monitor Attempted Calls	
Event Notification	
Raise event if attempted calls exceed threshold	Select **Yes** to raise an event if the number of attempted calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum attempted calls	Specify the highest number of calls that must be attempted before an event is raised. The default is 500.
Event severity when attempted calls exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of attempted calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for attempted calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls attempted during the monitoring period.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period.
Monitor Active Calls	
Data Collection	
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls active at each script iteration.
Monitor Calls In Progress	
Event Notification	

Parameter	How to Set It
Raise event if calls in progress exceed threshold	Select **Yes** to raise an event if the number of calls in progress exceeds the threshold you set. The default is Yes.
Threshold - Maximum calls in progress	Specify the highest number of calls that must be in progress before an event is raised. The default is 1000.
Event severity when calls in progress exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of calls in progress exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for calls in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls in progress at each script iteration.

H323_Trunk_CallActivity

Use this Knowledge Script to monitor attempted and completed calls for H.323 trunks. This script can raise an event if any threshold is exceeded. In addition, this script generates data streams for the following metrics:

- Completed calls per trunk
- Attempted calls per trunk
- Completed calls per cluster
- Attempted calls per cluster

Resource Object

Cluster object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity if job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the H323_Trunk_CallActivity job. The default is 5.
Monitor Attempted Calls	
Event Notification	
Raise event if attempted calls exceed threshold	Select **Yes** to raise an event if the number of attempted calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum attempted calls	Specify the highest number of calls that must be attempted before an event is raised. The default is 500.
Event severity when attempted calls exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of attempted calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for attempted calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls attempted during the monitoring period.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period.
Monitor Active Calls	
Data Collection	

Parameter	How to Set It
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls active at each script iteration.
Monitor Calls In Progress	
Event Notification	
Raise event if calls in progress exceed threshold	Select **Yes** to raise an event if the number of calls in progress exceeds the threshold you set. The default is Yes.
Threshold - Maximum calls in progress	Specify the highest number of calls that must be in progress before an event is raised. The default is 1000 calls.
Event severity when calls in progress exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of calls in progress exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for calls in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls in progress at each script iteration.

HealthCheck

Use this Knowledge Script to monitor the operational status of active services on Communications Manager servers. Although the script monitors the following services by default, you can choose to exclude any default service, or include any other service not mentioned in the list.

- A Cisco DB
- Cisco AMC Service
- Cisco CallManager
- Cisco CDR Agent
- Cisco CTL Provider
- Cisco Database Layer Monitor
- Cisco DRF Local
- Cisco Extension Mobility
- Cisco RIS Data Collector
- Cisco Tftp

This script raises an event if a stopped service is restarted or fails to restart, or if a service is stopped but the *Start service if it is stopped?* parameter has not been set to **Yes**. In addition, this script generates data streams for service availability.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 1172.

Resource Object

CiscoCM_CMServer

Default Schedule

By default, this script runs every two minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the HealthCheck job. The default is 5.
Monitor Services	
Default services to exclude	Type the name of any default service you do not want to automatically start. You can specify the names of multiple services, separated by commas.

Parameter	How to Set It
Other services to include	Type the name of any service you want to automatically start, but is not included in the list of default services. You can specify the names of multiple services, separated by commas.
Start service if it is stopped?	Select **Yes** to automatically start all stopped default services on Communications Manager servers. Any service you specify in *Default services to exclude* will not be started. The default is Yes. **Note** Only “activated” services can be automatically started. If an administrator has “deactivated” a service, then AppManager cannot start it.
Event Notification	
Raise event if service is stopped and should not be started?	Select **Yes** to raise an event if a monitored service is stopped but *Start service if it is stopped?* is unchecked. The default is Yes.
Event severity when service is stopped and should not be started	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service is stopped but *Start service if it is stopped?* is unchecked. The default is 15.
Raise event if service fails to start?	Select **Yes** to raise an event if AppManager cannot start a monitored service. The default is Yes.
Event severity when service fails to start	Set the event severity level, from 1 to 40, to indicate the importance of an event in AppManager cannot start a monitored service. The default is 5.
Raise event if stopped service has been started?	Select **Yes** to raise an event if AppManager successfully starts a monitored service. The default is Yes.
Event severity when stopped service has been started	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully starts a monitored service. The default is 25.
Raise event if service is deactivated?	Select **Yes** to raise an event if a monitored service has been deactivated by an administrator. The default is unselected.
Event severity when service is not active	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service has been deactivated by an administrator. The default is 15.
Data Collection	
Collect data for service availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns 0 for a stopped service or 1 for a started service. the default is Yes. **Note** This script generates data streams for services running when the job starts or automatically restarted while the job runs. If a service is deactivated when the job starts, no data stream is generated.

HuntAndRouteList

Use this Knowledge Script to monitor hunt lists and route lists for availability and call activity. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the number of abandoned calls, busy attempts, unanswered calls, active calls, in-progress calls, and available members, and for hunt and route list availability.

Resource Object

CiscoCM_HuntListObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the HuntAndRouteList job. The default is 5.
Monitor Abandoned Calls	
Event Notification	
Raise event if abandoned calls exceed threshold?	Select **Yes** to raise an event if the number of abandoned calls exceeds the threshold. The default is Yes.
Threshold - Maximum abandoned calls	Specify the maximum number of calls that must be abandoned before an event is raised. The default is 0 calls.
Event severity when abandoned calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of abandoned calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for abandoned calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls abandoned during the monitoring period.
Monitor Busy Attempts	
Event Notification	
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold. The default is Yes.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that must be detected to prevent an event from being raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold you set. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts that occurred during the monitoring period.
Monitor Unanswered Calls	
Event Notification	
Raise event if unanswered calls exceed threshold?	Select **Yes** to raise an event if the number of unanswered calls exceeds the threshold. The default is Yes.
Threshold - Maximum unanswered calls	Specify the maximum number of calls that must go unanswered before an event is raised. The default is 0 calls.
Event severity when unanswered calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of unanswered calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for unanswered calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that went unanswered during the monitoring period.
Monitor Active Calls	
Data Collection	
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls active at each script iteration.
Monitor Calls In Progress	
Data Collection	
Collect data for calls in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls in progress at each script iteration.
Monitor Hunt or Route List Availability	
Data Collection	
Collect data for hunt or route list availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the availability of a hunt or route list at each script iteration.
Monitor Members Available	
Data Collection	
Collect data for members available?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of hunt and route list members available at each script iteration.

Locations

Use this Knowledge Script to monitor Cisco locations for voice and video bandwidth availability and usage. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the bandwidth availability, bandwidth usage (%), bandwidth-related call failures, video bandwidth availability, video bandwidth usage (%), and bandwidth-related failures of video stream requests.

Resource Object

CiscoCM_LocationObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Locations job. The default is 5.
Monitor Available Bandwidth	
Data Collection	
Collect data for available bandwidth?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of bandwidth available at each script iteration.
Monitor Bandwidth Usage	
Event Notification	
Raise event if bandwidth usage exceeds threshold?	Select **Yes** to raise an event if the percentage of bandwidth usage exceeds the threshold. The default is Yes.
Threshold - Maximum bandwidth usage	Specify the maximum percentage of bandwidth usage that must be detected before an event is raised. The default is 90%.
Event severity when bandwidth usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of bandwidth usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for bandwidth usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of bandwidth usage at each script iteration.
Monitor Call Failures Caused By Insufficient Bandwidth	
Event Notification	
Raise event if call failures exceed threshold	Select **Yes** to raise an event if the number of calls that failed because of insufficient bandwidth exceeds the threshold. The default is Yes.
Threshold - Maximum failed calls	Specify the maximum number of calls that must fail before an event is raised. The default is 0 calls.

Parameter	How to Set It
Event severity when failed calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of call that failed because of insufficient bandwidth exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for failed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of call failures caused by insufficient bandwidth during the monitoring period.
Monitor Available Video Bandwidth	
Data Collection	
Collect data for available video bandwidth?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of video bandwidth available at each script iteration.
Monitor Video Bandwidth Usage	
Event Notification	
Raise event if video bandwidth usage exceeds threshold?	Select **Yes** to raise an event if the percentage of video bandwidth usage exceeds the threshold. The default is Yes.
Threshold - Maximum video bandwidth usage	Specify the maximum percentage of video bandwidth usage that must occur before an event is raised. The default is 90%.
Event severity when video bandwidth usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of video bandwidth usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for video bandwidth usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of video bandwidth usage at each script iteration.
Monitor Failed Video Stream Requests Caused by Insufficient Bandwidth	
Event Notification	
Raise event if failed video stream requests exceed threshold?	Select **Yes** to raise an event if the number of video stream requests that fail because of insufficient bandwidth exceeds the threshold. The default is Yes.
Threshold - Maximum failed video stream requests	Specify the maximum number of video stream requests that must fail before an event is raised. The default is 0 requests.
Event severity when failed video stream requests exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of video stream requests that fail because of insufficient bandwidth exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for failed video stream requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of bandwidth-related failures of video stream requests that occurred during the monitoring period.

MediaStreamingApp

Use this Knowledge Script to monitor the resources handled by the Media Streaming Application: annunciators, conference bridges, and Music-on-Hold (MOH) resources. This script raises an event if a threshold is exceeded. In addition, this script generates the following data streams:

- Lost Communications Manager connections
- Active and total annunciator streams
- Active and total software conferences
- Active and total software conference streams
- Active MOH audio sources
- Active and total MOH streams
- Active and total Media Termination Point streams

Resource Object

CiscoCM_MediaStreamingApp

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MediaStreamingApp job. The default is 5.
Monitor Lost CallManager Connections	
Event Notification	
Raise event if lost CallManager connections exceed threshold	Select **Yes** to raise an event if the number of lost Communications Manager connections exceeds the threshold. The default is Yes.
Threshold - Maximum lost CallManager connections	Specify the maximum number of Communications Manager connections that must be lost before an event is raised. The default is 0 connections.
Event severity when lost CallManager connections exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of lost Communications Manager connections exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for lost CallManager connections?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of Communications Manager connections lost during the monitoring period.
Monitor Active Annunciator Streams	

Parameter	How to Set It
Event Notification	
Raise event if active annunciator streams exceed threshold?	Select **Yes** to raise an event if the number of active annunciator streams exceeds the threshold you set. The default is Yes.
Threshold - Maximum active annunciator streams	Specify the maximum number of annunciator streams that can be active before an event is raised. The default is 200 streams.
Event severity when active annunciator streams exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active annunciator streams exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active annunciator streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of annunciator streams active at each script iteration.
Monitor Total Annunciator Streams	
Data Collection	
Collect data for total annunciator streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of annunciator streams during the monitoring period.
Monitor Active Software Conferences	
Event Notification	
Raise event if active software conferences exceed threshold?	Select **Yes** to raise an event if the number of active software conferences exceeds the threshold. The default is Yes.
Threshold - Maximum active software conferences	Specify the maximum number of software conferences that can be active before an event is raised. The default is 200 conferences.
Event severity when active software conferences exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active software conferences exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active software conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of software conferences active at each script iteration.
Monitor Total Software Conferences	
Data Collection	
Collect data for total software conferences?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of software conferences during the monitoring period.
Monitor Active Software Conference Streams	
Event Notification	
Raise event if active software conference streams exceed threshold?	Select **Yes** to raise an event if the number of active software conference streams exceeds the threshold you set. The default is Yes.
Threshold - Maximum active software conference streams	Specify the maximum number of software conference streams that can be active before an event is raised. The default is 500 streams.
Event severity when active software conference streams exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active software conference streams exceeds the threshold you set. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for active software conference streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of software conference streams active at each script iteration.
Monitor Total Software Conference Streams	
Data Collection	
Collect data for total software conference streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of software conference streams during the monitoring period.
Monitor Active Music-On-Hold Audio Sources	
Event Notification	
Raise event if active music-on-hold audio sources exceed threshold?	Select **Yes** to raise an event if the number of active MOH audio sources exceeds the threshold you set. The default is Yes.
Threshold - Maximum active music-on-hold audio sources	Specify the maximum number of MOH audio sources that can be active before an event is raised. The default is 200 sources.
Event severity when active music-on-hold audio sources exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active MOH audio sources exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active music-on-hold audio sources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MOH audio sources active at each script iteration.
Monitor Active Music-On-Hold Streams	
Event Notification	
Raise event if active music-on-hold streams exceed threshold?	Select **Yes** to raise an event if the number of active MOH streams exceeds the threshold you set. The default is Yes.
Threshold - Maximum active music-on-hold streams	Specify the maximum number of MOH streams that can be active before an event is raised. The default is 500 streams.
Event severity when active music-on-hold streams exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active MOH streams exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active music-on-hold streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MOH streams active at each script iteration.
Monitor Total Music-on-Hold Streams	
Data Collection	
Collect data for total music-on-hold streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of MOH streams during the monitoring period.
Monitor Active Media Termination Point Streams	
Event Notification	
Raise event if active media termination point streams exceed threshold?	Select **Yes** to raise an event if the number of active MTP streams exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum active media termination point streams	Specify the maximum number of MTP streams that can be active before an event is raised. The default is 500 streams.
Event severity when active media termination point streams exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active MTP streams exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active media termination point streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MTP streams active at each script iteration.
Monitor Total Media Termination Point Streams	
Data Collection	
Collect data for total media termination point streams?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of MTP streams during the monitoring period.

MGCP_FXO_CallActivity

Use this Knowledge Script to monitor completed calls, blocked calls, and outbound busy attempts on MGCP FXO (Media Gateway Control Protocol Foreign Exchange Office) devices. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the number of completed calls and busy attempts, percentage of blocked calls, and port status.

Resource Object

CiscoCM_MGCPFXSObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MGCP_FXO_CallActivity job. The default is 5.
Monitor Busy Attempts	
Event Notification	
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold. The default is Yes. A busy attempt is a call attempted when no voice channels are available.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that must be detected before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts that occurred during the monitoring period.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period.
Monitor Blocked Calls	
Data Collection	

Parameter	How to Set It
Collect data for blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of calls blocked during the monitoring period. AppManager computes the blocked call percentage as follows: (Outbound busy attempts delta x 100) / Total calls.
Monitor Ports Out of Service	
Data Collection	
Collect data for ports out of service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of ports out of service or that had an unknown status during the monitoring period.

MGCP_FXS_CallActivity

Use this Knowledge Script to monitor completed calls, blocked calls, and outbound busy attempts on MGCP FXS (Media Gateway Control Protocol Foreign Exchange Station) devices. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the number of completed calls and busy attempts, and for port status.

Resource Object

CiscoCM_MGCPFXSObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MGCP_FXS_CallActivity job. The default is 5.
Monitor Busy Attempts	
Event Notification	
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold. The default is Yes. A busy attempt is a call attempted when no voice channels are available.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that must be detected before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts that occurred during the monitoring period.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period.
Monitor Blocked Calls	
Data Collection	

Parameter	How to Set It
Collect data for blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of calls blocked during the monitoring period. AppManager computes the blocked call percentage as follows: (Outbound busy attempts delta x 100) / Total calls.
Monitor Ports Out of Service	
Data Collection	
Collect data for ports out of service?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of ports out of service or that had an unknown status during the monitoring period.

MGCP_GatewayUsage

Use this Knowledge Script to monitor active and in-service ports, active channels, and in-service spans for the following components of MGCP (Media Gateway Control Protocol) gateways:

- BRI (basic rate interface) spans
- FXO (foreign exchange office) ports
- FXS (foreign exchange station) ports
- PRI (primary rate interface) spans
- T1CAS (channel associated signaling) spans

An active port or channel is actively handling a call. An in-service port or span is registered to a Communications Manager and available for handling a call.

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for active ports and active channels.

Resource Object

CiscoCM_MGCPGatewayObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MGCP_GatewayUsage job. The default is 5.
Event Notification	
Raise event if number of BRI spans in service decreases?	Select **Yes** to raise an event if the number of in-service BRI spans has decreased since the last monitoring interval. The default is unselected.
Event severity when number of BRI spans in service decreases	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-service BRI spans has decreased since the last monitoring interval. The default is 15.
Raise event if number of FXO ports in service decreases?	Select **Yes** to raise an event if the number of in-service FXO ports has decreased since the last monitoring interval. The default is unselected.
Event severity when number of FXO ports in service decreases	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-service FXO ports has decreased since the last monitoring interval. The default is 15.

Parameter	How to Set It
Raise event if number of FXS ports in service decreases?	Select **Yes** to raise an event if the number of in-service FXS ports has decreased since the last monitoring interval. The default is unselected.
Event severity when number of FXS ports in service decreases	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-service FXS ports has decreased since the last monitoring interval. The default is 15.
Raise event if number of PRI spans in service decreases?	Select **Yes** to raise an event if the number of in-service PRI spans has decreased since the last monitoring interval. The default is unselected.
Event severity when number of PRI spans in service decreases	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-service PRI spans has decreased since the last monitoring interval. The default is 15.
Raise event if number of T1CAS spans in service decreases?	Select **Yes** to raise an event if the number of in-service T1CAS spans has decreased since the last monitoring interval. The default is unselected.
Event severity when number of T1CAS spans in service decreases	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-service T1CAS spans has decreased since the last monitoring interval. The default is 15.
Monitor Active BRI Channels	
Event Notification	
Raise event if active BRI channels exceed threshold?	Select **Yes** to raise an event if the number of active BRI channels exceeds the threshold. The default is Yes.
Threshold - Maximum active BRI channels	Specify the maximum number of BRI channels that must be active before an event is raised. The default is 25 channels.
Event severity when active BRI channels exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active BRI channels exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active BRI channels?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of BRI channels active at each script iteration.
Monitor Active FXO Ports	
Event Notification	
Raise event if active FXO ports exceed threshold?	Select **Yes** to raise an event if the number of active FXO ports exceeds the threshold. The default is Yes.
Threshold - Maximum active FXO ports	Specify the maximum number of FXO ports that must be active before an event is raised. The default is 100 ports.
Event severity when active FXO ports exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active FXO ports exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active FXO ports?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of FXO ports active at each script iteration.
Monitor Active FXS Ports	
Event Notification	
Raise event if active FXS ports exceed threshold?	Select **Yes** to raise an event if the number of active FXS ports exceeds the threshold. The default is Yes.

Parameter	How to Set It
Threshold - Maximum active FXS ports	Specify the maximum number of FXS ports that must be active before an event is raised. The default is 100 ports.
Event severity when active FXS ports exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active FXS ports exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active FXS ports?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of FXS ports active at each script iteration.
Monitor Active PRI Channels	
Event Notification	
Raise event if active PRI channels exceed threshold?	Select **Yes** to raise an event if the number of active PRI channels exceeds the threshold. The default is Yes.
Threshold - Maximum PRI channels	Specify the maximum number of PRI channels that must be active before an event is raised. The default is 100 channels.
Event severity when active PRI channels exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active PRI channels exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active PRI channels?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of PRI channels active at each script iteration.
Monitor Active T1CAS Channels	
Event Notification	
Raise event if active T1CAS channels exceed threshold?	Select **Yes** to raise an event if the number of active T1CAS channels exceeds the threshold. The default is Yes.
Threshold - Maximum T1CAS channels	Specify the maximum number of T1CAS channels that must be active before an event is raised. The default is 100 channels.
Event severity when active T1CAS channels exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active T1CAS channels exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active T1CAS channels?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of T1CAS channels active at each script iteration.

MGCP_PRI_CallActivity

Use this Knowledge Script to monitor active calls, completed calls, blocked calls, outbound busy attempts, and data link availability on an MGCP PRI (Media Gateway Control Protocol Primary Rate Interface) device. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following metrics:

- Active calls
- Completed calls
- Busy attempts
- Blocked calls

Resource Object

CiscoCM_MGCPPRIObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MGCP_PRI_CallActivity job. The default is 5.
Event Notification	
Raise event if Data Link out of service?	Select **Yes** to raise an event if any data link is unavailable. The default is Yes.
Event severity when Data Link out of service	Set the event severity level, from 1 to 40, to indicate the importance of an event in which any data link is unavailable. The default is 5.
Monitor Busy Attempts	
Event Notification	
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold. The default is Yes. A busy attempt is a call attempted when no voice channels are available.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that must be detected before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts that occurred during the monitoring period.

Parameter	How to Set It
Monitor Active Calls	
Data Collection	
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls active during the monitoring period.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period.
Monitor Blocked Calls	
Data Collection	
Collect data for blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of calls blocked during the monitoring period. AppManager computes the blocked call percentage as follows: (Outbound busy attempts delta x 100) / Total calls.

MGCP_PRI_ChannelHealth

Use this Knowledge Script to monitor the status of channels for an MGCP PRI (Media Gateway Control Protocol Primary Rate Interface) device. This script raises an event if a channel is not available.

Resource Object

CiscoCM_MGCPPRIObj

Default Schedule

By default, this script runs every two minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MGCP_PRI_ChannelHealth job. The default is 5.
Monitor PRI Channels	
Select PRI channels to monitor	Select one or more PRI channels to monitor. To monitor all channels, select **All**. To select individual channels in the list, press `[Ctrl]` while clicking on the channels you want. To select an entire range of channels, press `[Shift]` while clicking on the first and last channel in the range.
Treat unknown channel status as out-of-service	Select **Yes** to classify as out-of-service any selected channel whose status is unknown. The default is unselected. An out-of-service channel will trigger this script to raise an event.
Event Notification	
Raise event if channel is not available?	Select **Yes** to raise an event if the selected PRI channels are not available. The default is Yes.
Event severity when channel is not available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which at least one of the selected PRI channels is not available. The default is 5.

MGCP_T1CAS_CallActivity

Use this Knowledge Script to monitor active calls, completed calls, blocked calls, and outbound busy attempts on an MGCP T1CAS (Media Gateway Control Protocol Channel Associated Signaling) device. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following metrics:

- Active calls
- Completed calls
- Blocked calls
- Busy attempts

Resource Object

CiscoCM_MGCPT1CASObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MGCP_T1CAS_CallActivity job. The default is 5.
Monitor Busy Attempts	
Event Notification	
Raise event if busy attempts exceed threshold?	Select **Yes** to raise an event if the number of busy attempts exceeds the threshold. The default is Yes. A busy attempt is a call attempted when no voice channels are available.
Threshold - Maximum busy attempts	Specify the maximum number of busy attempts that must be detected before an event is raised. The default is 0 attempts.
Event severity when busy attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of busy attempts exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for busy attempts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of busy attempts that occurred during the monitoring period.
Monitor Active Calls	
Data Collection	
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls active during the monitoring period.

Parameter	How to Set It
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period.
Monitor Blocked Calls	
Data Collection	
Collect data for blocked calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of calls blocked during the monitoring period. AppManager computes the blocked call percentage as follows: (Outbound busy attempts delta x 100) / Total calls.

MGCP_T1CAS_ChannelHealth

Use this Knowledge Script to monitor the status of channels for an MGCP T1CAS (Media Gateway Control Protocol Channel Associated Signaling) device. This script raises an event if a channel is not available.

Resource Object

CiscoCM_MGCPT1CASObj

Default Schedule

By default, this script runs every two minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MGCP_T1CAS_ChannelHealth job. The default is 5.
Monitor T1CAS Channels	
Select T1CAS channels to monitor	Select one or more T1CAS channels to monitor. To monitor all channels, select **All**. To monitor selected channels, press `[Ctrl]` while clicking on the channels you want.
Treat unknown channel status as out-of-service?	Select **Yes** to classify as out-of-service any selected channel whose status is unknown. The default is unselected. An out-of-service channel will trigger this script to raise an event.
Event Notification	
Raise event if channel is not available?	Select **Yes** to raise an event if the selected T1CAS channels are not available. The default is Yes.
Event severity when channel is not available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the selected T1CAS channels are not available. The default is 5.

MOH_Device

Use this Knowledge Script to monitor the resource usage for a registered Music-on-Hold (MOH) device. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for multicast resource usage (%), active multicast resources, unicast resource usage (%), active unicast resources, and resource availability.

Resource Object

CiscoCM_MOH_DeviceObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MOH_Device job. The default is 5.
Monitor Multicast Resource Usage	
Event Notification	
Raise event if multicast resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of multicast resource usage exceeds the threshold. The default is Yes.
Threshold - Maximum multicast resource usage	Specify the maximum percentage of multicast resource usage that must be detected before an event is raised. The default is 80%.
Event severity when multicast resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of multicast resource usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for multicast resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of multicast resource at each script iteration.
Monitor Active Multicast Resources	
Data Collection	
Collect data for active multicast resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of multicast resources active at each script iteration.
Monitor Unicast Resource Usage	
Event Notification	
Raise event if unicast resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of unicast resource usage exceeds the threshold. The default is Yes.

Parameter	How to Set It
Threshold - Maximum unicast resource usage	Specify the maximum percentage of unicast resource usage that must be detected before an event is raised. The default is 80%.
Event severity when unicast resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of unicast resource usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for unicast resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of unicast resource usage at each script iteration.
Monitor Active Unicast Resources	
Data Collection	
Collect data for active unicast resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of unicast resources active at each script iteration.
Monitor Unavailable Resources	
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times MOH resources were unavailable exceeds the threshold. The default is Yes.
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times MOH resources can be unavailable before an event is raised. The default is 0 instances.
Event severity when number of times resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of unavailability instances exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times MOH resources were unavailable during the monitoring period.

MTP_Device

Use this Knowledge Script to monitor the resource usage for a registered Media Termination Point (MTP) device. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for resource usage (%), active resources, and resource availability.

Resource Object

CiscoCM_MTP_DeviceObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MTP_Device job. The default is 5.
Monitor Resource Usage	
Event Notification	
Raise event if resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of MTP resource usage exceeds the threshold. The default is Yes.
Threshold - Maximum resource usage	Specify the maximum percentage of MTP resource usage that must be detected before an event is raised. The default is 80%.
Event severity when resource usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of MTP resource usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of MTP resource usage at each script iteration.
Monitor Active Resources	
Data Collection	
Collect data for active resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of MTP resources active at each script iteration.
Monitor Unavailable Resources	
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times MTP resources were unavailable exceeds the threshold. The default is Yes.

Parameter	How to Set It
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times MTP resources can be unavailable before an event is raised. The default is 0 instances.
Event severity when number of times resources were unavailable exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times MTP resources were unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times MTP resources were unavailable during the monitoring period.

PhoneDeregistrations

Use this Knowledge Script to monitor phone deregistrations on a Unified Communications Manager and to maintain a history of phone deregistrations in the Cisco CM supplemental database. This script raises an event if the number or percentage of lost phones exceeds the threshold you set. You determine how long a phone must be deregistered before it is considered "lost." In addition, you determine whether to group the events by cluster, device pool, location, or partition.

Unified Communications Manager reports a phone as deregistered even after that phone has been deleted from Communications Manager configuration, unplugged, and moved to a different cluster. As long as Unified Communications Manager indicates the phone is deregistered, AppManager continues to raise an event that identifies the deregistered phone. When Unified Communications Manager stops reporting the phone as deregistered, three days after the phone has been deleted, AppManager stops raising a "deregistered" event.

Prerequisites

- Run the SetupSupplementalDB Knowledge Script to create the Cisco CM supplemental database that will house the deregistration data.
- Run the CDR_RetrieveCallRecords and CDR_RetrieveConfigData Knowledge Scripts to populate the database.

For more information, see "Understanding the Cisco CM Supplemental Database" on page 1144.

Resource Object

CiscoCM_CDRMgmt

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the PhoneDeregistrations job. The default is 5.
Event Notification	
Raise event if lost phones in group exceed threshold?	Select **Yes** to raise an event if the number or percentage of lost phones in a group exceeds the threshold you set. The default is Yes. Use *Select event grouping* to select how to group the lost phones. Use *Maximum time phone deregistered before counted as lost* to determine how long a phone must be deregistered before it is considered lost.

Parameter	How to Set It
Select event grouping	Select whether to group lost phones by **Cluster**, **Device Pool**, **Location**, or **Partition**. AppManager raises an event based on whether the number of lost phones in *each* group exceeds the threshold you set. For example, you set *Maximum number of lost phones in the group* to 5, you set *Select event grouping* to Device Pool, and you have three device pools. If AppManager detects six lost phones in the first pool, two in the second, and seven in the third, it will raise two events: one for the six lost phones in the first pool and another for the seven lost phones in the third pool. Because you set the threshold to "5," no event is raised for the lost phones in the second pool. The default is Cluster.
Maximum time phone deregistered before counted as lost	Specify the number of minutes that must elapse before a deregistered phone can be considered a "lost" phone. The default is 0 minutes. Accept the default if you want *all* deregistered phones to be considered lost.
Type of threshold	Select whether you want to raise events based on the **Number** or **Percent** of lost phones. The default is Number.
Threshold - Maximum number of lost phones	Use this parameter if you selected **Number** in *Type of threshold*. Specify the maximum number of phones that can be lost before an event is raised. The default is 0.
Threshold - Maximum percent of lost phones	Use this parameter if you selected **Percent** in *Type of threshold*. Specify the maximum percentage of phones that can be lost before an event is raised. The default is 0.
Event severity when lost phones exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number or percentage of lost phones in a group exceeds the threshold you set. The default is 15.
Include lost phone details in event message	Select **Yes** to include details of the lost phones in the event message. Phone details can include device name, device IP address, directory number, description, name of device pool, time of deregistration, and the Communications Manager from which the phone was deregistered. The default is Yes.
Maximum number of detail rows to include in event detail	Specify the maximum number of detail rows to include in an event message. Each row contains details for one phone. Rows are sorted in order by most recently lost phone. Specify "0" to include all rows. The default is 20. This parameter is applicable only if you selected **Yes** for *Include lost phone details in event message*.

PhoneInventory

Use this Knowledge Script to create an inventory of the phones configured in a Communications Manager cluster. You choose both the search criteria for the inventory and the location of the output folder (for the results file containing the inventory list). Unless you specify a UNC path (`\\servername\sharename\directoryname\filename`), the results file is written to the computer on which the NetIQ AppManager agent is running. If you specify a UNC path, ensure the `NetIQmc` service is running as an account that has the proper permissions on the UNC path.

Monitoring Phone Registration After Failover

You can determine the status, registered or deregistered, of Communications Manager phones for Unified Communications Manager clusters on which failover has occurred. Failover occurs when Communications Manager status changes from Primary to Backup.

Communications Managers that fail over contain only a list of phones that registered since failover occurred. They do not provide a list of phones that deregistered as a result of failover. To determine which phones have deregistered, use the PhoneInventory Knowledge Script.

To determine whether failover has occurred, use the RoleStatus or CCM_RegisteredResources script.

Resource Object

CiscoCM_Devices

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the PhoneInventory job. The default is 5.
Raise event if phone inventory succeeds?	Select **Yes** to raise an event when a phone inventory file is successfully generated. The default is Yes.
Event severity when phone inventory succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the inventory file is successfully generated. The default is 25.
Raise event if no records found?	Select **Yes** to raise an event when the PhoneInventory job finds no phones based on the criteria you selected. The default is Yes.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the PhoneInventory job found no phones based on the criteria you selected. The default is 25.
Search Options	

Parameter	How to Set It
Select by	Choose the type of selection criteria you want to use to create the list of phones. • Name (the default) • DirectoryNumber. If you select this option, you must also enable the *Include directory number and partition columns in report?* parameter. • Description • DevicePool • CallingSearchSpace • Location • Partition. If you select this option, you must also enable the *Include directory number and partition columns in report?* parameter. • Subnet. If you select this option, you must enter the subnet address in the *Selection criteria* parameter. Use the following format: `172.16.10.0/20` • SubnetFilepath. If you select this option, then, in the *Selection criteria* parameter, enter the UNC or full path to a file on the agent computer that contains a list of subnet specifications. The file must be located on the agent computer.
Selection criteria	Type the selection criteria for the phones to be listed. You can specify the actual item or you can specify a pattern by using the * wildcard. For example, to monitor all the phones with device names that begin with SEP, enter `SEP*`. You can enter multiple items by separating each item with a comma. For example: `SEP0009A*,SEP0009B*` The items you enter must be of the same type as the *Select by* parameter. So if *Select by* is Name, then the items you enter must be device names or patterns. If *Select by* is DirectoryNumber, then the items you enter must be directory numbers or patterns.
List only phones with status of	To further filter the list of phones, select a status. Only phones of this status type, matching the criteria you specified in *Selection criteria* and *Select by*, will be included in the inventory list. Select from the following status types: • Any • Not Registered • Registered • Unregistered • Rejected **Note** Setting this parameter to a value of **Not Registered** will also list those phones with a status of **Unregistered**.
Result File Options	
Full path to output folder for result file	Type the full path or a UNC path to a location on the agent computer in which to save the inventory `.csv` file. The default path is `c:\Program Files\NetIQ\Temp\NetIQ_Debug\PhoneInventory.csv`

Parameter	How to Set It
Order by	Select **Name** to display the contents of the results file in order by phone name. The default is Name. Select **DirectoryNumber** to display the contents of the results file in order by directory numbers. If you select DirectoryNumber, also enable the *Include directory number and partition columns in report?* parameter.
Include directory number and partition columns in report?	Because a phone can be associated with multiple directory numbers and partitions, your inventory report can present the same phone several times, once for each directory number or partition. Select **Yes** to include the directory number and partition columns in the inventory, allowing multiple entries per phone. Disable this option to remove the directory number and partition columns from the inventory, allowing only one entry per phone. **Note** You must select **Yes** if you selected any of the following parameter options: • The *Select by* parameter is set to **DirectoryNumber** or **Partition**. • The *Order by* parameter is set to **DirectoryNumber**.

Report_PhoneDeregAudit

Use this Knowledge Script to create a history of phone deregistrations and reregistrations. This script uses the data stored in the Cisco CM supplemental database and collected by the PhoneDeregistrations script.

The completed Phone Deregistrations Audit report contains a column titled "Entry Type." In this column, you may occasionally see an entry of "Reregister - Missed." This entry indicates a phone that has, apparently, deregistered and then reregistered within a single iteration of this script. AppManager can tell something happened because the timestamp on the reregistration is different from the last time the phone was polled. However, because the phone is registered, AppManager is unable to determine exactly what transpired.

Prerequisite

For the AppManager for Cisco Unified Communications Manager module, the Report agent pulls data from the Cisco CM supplemental database rather than from the AppManager repository. The `netiqmc` service on the Report agent computer must be running as an account that has permission to access the supplemental database you created using the SetupSupplementalDB Knowledge Script. The Report agent and supplemental database need to be located on the same computer for the PhoneDeregAudit report to work.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select cluster	Select the Communications Manager cluster for which you want to create a deregistered phone audit report.
Cisco CM SQL instance	Specify the SQL instance that contains the Cisco CM supplemental database from which the report should pull data. Use the same SQL instance you specified in the PhoneDeregistrations script parameters. Leave this parameter blank to accept the default instance.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Search Criteria	

Note for entering search criteria: If you enter only the wildcard (*) for a field (such as Partition name), then AppManager matches *only* those deregistered phones that have a value for that field. Phones for which that field has no value (i.e., is NULL) will not be matched. For example, if you enter * in the "Partition name" parameter, then the search matches only those phones that have been configured for some partition name. To match all deregistered phones (including phones that have no value for the selected field), leave the search criteria parameter blank.

Parameter	How to Set It
Directory number	Type the directory number for which you want to identify phone deregistrations.
Device name	Type the name of the device for which you want to identify phone deregistrations.
Device IP address	Type the IP address of the device for which you want to identify phone deregistrations. You can use one of the following formats: • Single dotted-decimal IP address, such as 10.41.2.31 • Dotted-decimal IP address that includes a wildcard, such as 10.41.*.*, which would search for all IP addresses in the range of 10.41.0.0 to 10.41.255.255. • Range of dotted-decimal IP addresses separated by a hyphen, such as 10.41.2.31-10.41.2.41. The first address indicates the beginning of the range; the second IP address marks the end of the range.
Device pool	Type the name of the device pool for which you want to identify phone deregistrations.
Location	Type the name of the device location for which you want to identify phone deregistrations. **Note** The device location is the location configured on the Communications Manager.
Partition name	Type the name of the partition for which you want to identify phone deregistrations.
Report Settings	
Order rows by?	Select the column by which you want to sort the rows in the report. The default is DeregTimeDescending.
Show outage time in minutes or seconds?	Select whether the Outage Time column of the report displays the deregistration period in **Minutes** or **Seconds**. The default is Minutes. The outage time is calculated as the difference between the time of deregistration and the time of reregistration.
Include parameter help card?	Select y to include a table in the report that lists parameter settings for this script. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is PhoneDeregistrationAudit.
Add job ID to output folder name?	Select y to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Phone Deregistration Audit.
Add time stamp to title?	Select y to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Select y to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.

Parameter	How to Set It
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_PhoneDeregWatchList

Use this Knowledge Script to create a list of phones that deregister frequently. This script uses the data stored in the Cisco CM supplemental database and collected by the PhoneDeregistrations script.

Prerequisite

For the AppManager for Cisco Unified Communications Manager module, the Report agent pulls data from the Cisco CM supplemental database rather than from the AppManager repository. The `netiqmc` service on the Report agent computer must be running as an account that has permission to access the supplemental database you created using the SetupSupplementalDB Knowledge Script. The Report agent and supplemental database need to be located on the same computer for the PhoneDeregWatchList report to work.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select cluster	Select the Communications Manager cluster for which you want to create a deregistered phone report.
Cisco CM SQL instance	Specify the SQL instance that contains the Cisco CM supplemental database from which the report should pull data. Use the same SQL instance you specified in the PhoneDeregistrations script parameters.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Search Criteria	
Note for entering search criteria: If you enter only the wildcard (*) for a field (such as Partition name), then AppManager matches *only* those deregistered phones that have a value for that field. Phones for which that field has no value (i.e., is NULL) will not be matched. For example, if you enter * in the "Partition name" parameter, then the search matches only those phones that have been configured for some partition name. To match all deregistered phones (including phones that have no value for the selected field), leave the search criteria parameter blank.	
Minimum number of deregistrations	Specify the minimum number of deregistrations that must have occurred on a phone before that phone is included in the deregistration report. For example, if you specify "5" as the minimum, then any phone that has four or fewer deregistrations is not included in the report.
Directory number	Type the directory number for which you want to watch phone deregistrations.
Device name	Type the name of the device for which you want to watch phone deregistrations.

Parameter	How to Set It
Device IP address	Type the IP address of the device for which you want to watch phone deregistrations. You can use one of the following formats: • Single dotted-decimal IP address, such as 10.41.2.31 • Dotted-decimal IP address that includes a wildcard, such as 10.41.*.*, which would search for all IP addresses in the range of 10.41.0.0 to 10.41.255.255. • Range of dotted-decimal IP addresses separated by a hyphen, such as 10.41.2.31-10.41.2.41. The first address indicates the beginning of the range; the second IP address marks the end of the range.
Device pool	Type the name of the device pool for which you want to watch phone deregistrations.
Location	Type the name of the device location for which you want to watch phone deregistrations. **Note** The device location is the location that is configured on the Communications Manager.
Partition name	Type the name of the partition for which you want to watch phone deregistrations.
Report Settings	
Order rows by?	Select the column by which you want to sort the rows in the report. The default is Deregistrations.
Include parameter help card?	Select y to include a table in the report that lists parameter settings for this script. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is PhoneDeregistrationWatchList.
Add job ID to output folder name?	Select y to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set miscellaneous report properties as desired. The default report name is Phone Deregistration Watch List.
Add time stamp to title?	Select y to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Select y to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

RoleStatus

Use this Knowledge Script to monitor a Communications Manager group for changes in the status of its primary and backup Communications Managers. This script raises an event if the initial status of the primary Communications Manager is "not active." In addition, this script raises an event if the status of the primary or backup Communications Manager changes.

Resource Object

CiscoCM_CMGroupObj

Default Schedule

By default, this script runs every five minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the RoleStatus job. The default is 5.
Event Notification	
Raise event if primary CallManager is not active?	Select **Yes** to raise an event if the primary Communications Manager is not active when you start the RoleStatus job. The default is unselected.
Event severity when primary CallManager is not active	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the primary Communications Manager is not active when you start the RoleStatus job. The default is 5.
Raise event if primary CallManager status changes?	Select **Yes** to raise an event if the status of the primary Communications Manager changes while the RoleStatus job is running. The default is Yes.
Event severity when primary CallManager status changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of the primary Communications Manager changes while the RoleStatus job is running. The default is 5.
Raise event if backup CallManager status changes?	Select **Yes** to raise an event if the status of the backup Communications Manager changes while the RoleStatus job is running. The default is Yes.
Event severity when backup CallManager status changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of the backup Communications Manager changes while the RoleStatus job is running. The default is 5.

SetupSupplementalDB

Use this Knowledge Script to verify that Communications Manager is properly configured for the collection of Call Detail Records (CDRs). This script creates a Cisco CM supplemental database, plus the tables and stored procedures needed to store CDRs. In addition, this script creates a SQL job that removes old records from the supplemental database.

Understanding the Cisco CM Supplemental Database

The Cisco CM supplemental database is a SQL Server database you create on the proxy agent computer. The supplemental database fulfills three functions:

- **Storage for CDRs.** The Unified Communications Manager server pushes CDRs, which are flat files, to a folder on the proxy agent computer. From there, the CDRs are saved to tables in the Cisco CM supplemental database, from which the CDR_CallFailures, CDR_CallQuality, and CDR_Query Knowledge Scripts can easily monitor and retrieve data.

  When you create the supplemental database, you specify how long data is retained before being deleted and archived. AppManager automatically archives any flat files older than the retention age you specify. That way, no time or CPU is wasted by transferring to the supplemental database any files that will be immediately slated for deletion.

- **Data source for Call Data Analysis module.** By creating a supplemental database in which to store CDRs, you establish a means of using the AppManager for Call Data Analysis module for analyzing call activity for Unified Communications Manager. The Call Data Analysis module was designed to analyze CDRs that are pushed to a supplemental database. The CDR_RetrieveConfigData script retrieves the Unified Communications Manager configuration information Call Data Analysis requires and stores it in the supplemental database.

  When using AppManager for Call Data Analysis, simply identify the Cisco CM supplemental database as a Data Source when you run the CallDataAnalysis_AddDataSource_CiscoCM Knowledge Script.

- **Storage for phone deregistration data.** The PhoneDeregistrations Knowledge Script uses AXL queries to create a list of unregistered phones and to identify when they reregister. The script stores the deregistration data in an audit table in the Cisco CM supplemental database, from which it is easily accessed for reporting. The CDR_RetrieveConfigData script retrieves the Communications Manager configuration information the Report scripts need to accommodate your grouping choices and stores it in the supplemental database.

To use the supplemental database:

1. **Create the database**. Use the SetupSupplementalDB Knowledge Script to create one Cisco CM supplemental database per Unified Communications Manager cluster you are monitoring.

2. **Populate the database**. Use CDR_RetrieveConfigData to retrieve configuration data from Unified Communications Manager and save it to the Cisco CM supplemental database. Then run CDR_RetrieveCallRecords to retrieve the CDR flat files from the folder into which they were pushed (using FTP) by the primary Communications Manager. This folder is located on the proxy agent computer; you configure the primary Communications Manager to send CDRs to this location.

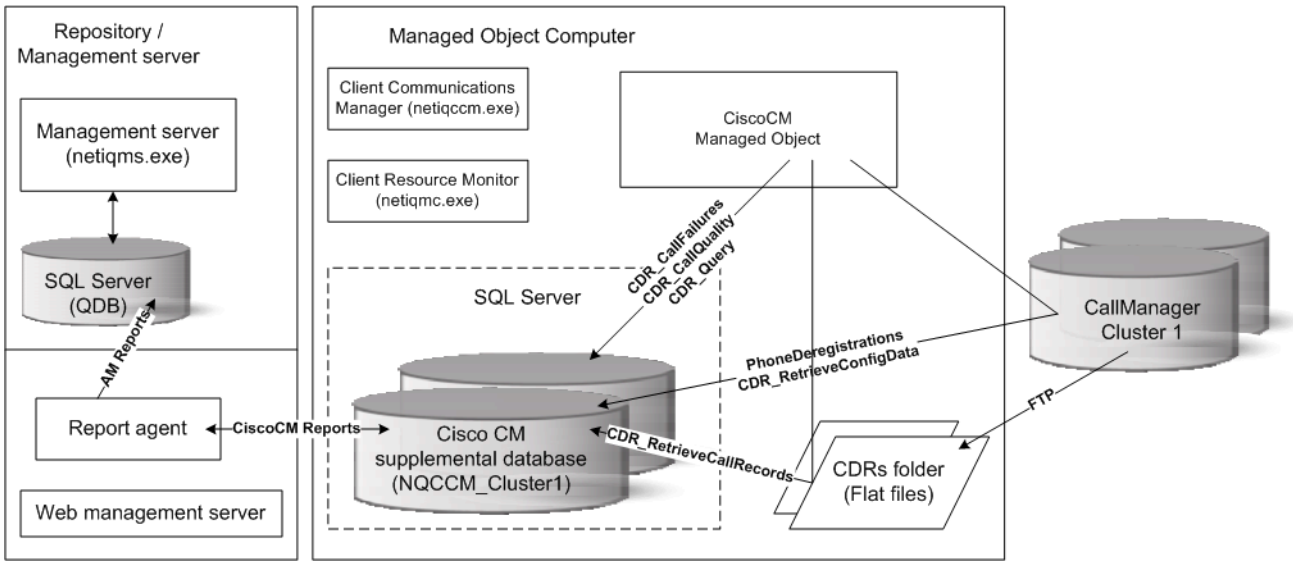
   Although the PhoneDeregistrations script does not monitor data in the supplemental database, it does populate the audit table in the database with phone deregistration data, which is subsequently used by the Report_PhoneDeregAudit and Report_PhoneDeregWatchList Report scripts.

3. **Monitor the data in the database**. Depending on your monitoring objectives, use the following scripts to analyze the data in the database.

- CDR_CallFailures monitors CDRs for calls that ended with an abnormal termination code.
- CDR_CallQuality monitors CDRs for jitter, latency, lost data, and MOS.
- CDR_Query searches CDRs based on query filters you select.
- PhoneDeregistrations monitors phone deregistrations and maintains a history of phone deregistrations in the supplemental database

4. **Run the Report Knowledge Scripts**. The Report_PhoneDeregAudit and Report_PhoneDeregWatchList scripts organize and display the information in the Cisco CM supplemental database. The reporting function requires the `netiqmc` service on the Report agent computer to be running as an account that has permissions on the supplemental database.

The following diagram illustrates the flow of data between the supplemental database and the various components of AppManager for Cisco Unified Communications Manager:



Resource Object

CiscoCM CDR Mgmt

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SetupSupplementalDB job. The default is 5.
Phone Deregistration Parameters	

Parameter	How to Set It
Number of days to keep phone deregistration audit entries	Specify the number of days' worth of phone deregistration audit entries you want to keep in the Cisco CM supplemental database. Any data older than what you specify is discarded. The default is 180 days.
CDR Parameters	
Full path to call detail records	Specify the full path to the location of the CDRs on the proxy agent computer. The TreeView cluster name must appear in the path. Use the same TreeView cluster name you used when configuring the proxy agent computer as a billing server. For example, *if* you entered `CCM80-01\` as the host name of the primary server when you configured the billing server *and* your FTP server is installed in the default location, then enter the following: `c:\inetpub\ftproot\CCM80-01`
Number of days to keep call detail records	Specify the number of days' worth of call detail records you want to keep in the Cisco CM supplemental database. Any data older than what you specify is discarded. The default is 7 days.
SQL Server Information	
Local SQL Server Instance name	Specify the name of the local SQL Server instance (on the proxy agent computer) in which you want to create the new Cisco CM supplemental database. Leave this parameter blank to accept the default name.
Raise event if database setup succeeds?	Select **Yes** to raise an event if the setup of the Cisco CM supplemental database is successful. The default is unselected.
Event severity when database setup succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the success of the setup of the Cisco CM supplemental database. The default is 25.

SIP_Trunk_CallActivity

Use this Knowledge Script to monitor attempted, completed, in-progress, and active calls for SIP trunks. This script raises an event if any threshold is exceeded. In addition, this script generates data streams for the following metrics:

- Attempted calls per trunk
- Completed calls per trunk
- In-progress calls per trunk
- Active calls per trunk

Resource Object

SIPTrunk object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity if job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SIP_Trunk_CallActivity job. The default is 5.
Monitor Attempted Calls	
Event Notification	
Raise event if attempted calls exceed threshold	Select **Yes** to raise an event if the number of attempted calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum attempted calls	Specify the highest number of calls that must be attempted before an event is raised. The default is 500.
Event severity when attempted calls exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of attempted calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for attempted calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were attempted during the monitoring period.
Monitor Completed Calls	
Data Collection	
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were completed during the monitoring period.
Monitor Active Calls	
Data Collection	

Parameter	How to Set It
Collect data for active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that are active at each script iteration.
Monitor Calls In Progress	
Event Notification	
Raise event if calls in progress exceed threshold	Select **Yes** to raise an event if the number of calls in progress exceeds the threshold that you set. The default is Yes.
Threshold - Maximum calls in progress	Specify the highest number of calls that must be in progress before an event is raised. The default is 1000.
Event severity when calls in progress exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of calls in progress exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for calls in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that are in progress at each script iteration.

SNMPTrap_AddMIB

Use this Knowledge Script to add MIB (management information base) files to the MIB tree that is monitored by the SNMPTrap_Async Knowledge Script. The MIB files should be `ASN.1` text file with a `.txt` or `.my` file extension, and not compiled MIB files.

With this script you can copy a MIB file from an arbitrary directory to the MIB tree located in the `<AppManager directory>\bin\MIBs` directory. And, by using the *Reload MIB tree?* parameter, you can also reload all MIBs in the tree without restarting the AppManager agent. A restart of the AppManager agent automatically reloads the MIB tree, a directory of MIBs.

Scenarios for using this script include the following examples:

In This Scenario	Set These Parameters
You want to add a MIB file to the MIB tree, but do not want the addition to take effect until after the next restart of the AppManager agent.	*Full path to MIB files* and *List of MIB files*: Provide location and name of MIB file you want to add. *Reload MIB tree?*: Select **No** (unchecked).
You manually copied a MIB file to the MIB directory and want to reload all MIBs in the tree.	*Full path to MIB files* and *List of MIB files*: Leave blank. *Reload MIB tree?*: Select **Yes**. *MIB reload timeout*: Set new timeout value or accept default of 10 seconds.
Due to compiler errors, you edited some MIBs in the MIB directory. Now you want to reload the MIBs to ensure the errors have been fixed.	*Full path to MIB files* and *List of MIB files*: Leave blank. *Reload MIB tree?*: Select **Yes**. *MIB reload timeout*: Set new timeout value or accept default of 10 seconds.

For more information, see "Working with NetIQ SNMP Trap Receiver" on page 1152.

Resource Object

CiscoCM_TrapReceiver

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Full path to MIB files	Specify the full path to the folder that contains the MIB files you want to install. The AppManager agent on the proxy computer must have SNMP access to the location you specify.
List of MIB files	Type a comma-separated list of the MIB files you want to install. The MIB files should be `ASN.1` text files with a `.TXT` or `.MY` file extension. The MIB files should not be compiled MIB files. The MIB files you specify must be located in the folder you identified in the *Full path to MIB files* parameter.
Reload MIB tree?	Select **Yes** to update the MIB tree.

Parameter	How to Set It
MIB reload timeout	Specify the length of time AppManager should attempt to update the MIB tree before timing out and raising a failure event. The default is 10 seconds.
Event Notification	
Raise event if installation and reloading of MIB tree succeeds?	Select **Yes** to raise an event if installation of the MIB files and/or reloading of the MIB tree succeeds. The default is Yes. Note that reloading of the MIB tree can be successful even if no new MIB files are installed. Reloading of the MIB tree can proceed even if you provide no MIB files in the *List of MIB files* or *Full path to list of MIB files* parameters.
Event severity when installation and reloading of MIB tree succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the installation of MIB files and/or the reloading of the MIB tree succeeds. The default is 25.
Raise event if "reload MIB parser" warnings received?	Select **Yes** to raise an event if warning messages are received during the reload process. The default is Yes. Warning scenarios include: • MIBs are installed successfully but the *Reload MIB tree?* parameter is not set to Yes. • Not all specified MIB files were loaded to the MIB tree.
Event severity when "reload MIB parser" warnings received	Set the severity level, from 1 to 40, to indicate the importance of an event in which warning messages are received during the reload process. The default is 15.
Raise event if installation and reloading of MIB tree fails?	Select **Yes** to raise an event if AppManager fails to install or reload the specified MIB files. The default is Yes. Failure scenarios include: • MIB reload timeout period expired. • Not all specified MIB files were installed.
Event severity when installation and reloading of MIB tree fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the installation or reloading of the MIB tree fails. The default is 10.
Raise event with the list of currently installed MIBs?	Select **Yes** to raise an informational event that provides a list of all MIBs installed in the MIB tree. The default is Yes.
Event severity for list of currently installed MIBs	Set the severity level, from 1 to 40, to indicate the importance of an event that provides a list of all MIBs installed in the MIB tree. The default is 25.

SNMPTrap_Async

Use this Knowledge Script to check for SNMP traps forwarded from NetIQ SNMP Trap Receiver. This script raises an event when an SNMP trap is received and when Trap Receiver is unavailable or subsequently becomes available. In addition, this script generates data streams for Trap Receiver availability.

This script checks for SNMP traps in the MIB tree. You can add Management Information Bases (MIBs) to the MIB tree. For more information, see the SNMPTrap_AddMIB Knowledge Script.

In general, a trap receiver is an application that receives traps from SNMP agents. NetIQ SNMP Trap Receiver (Trap Receiver) receives SNMP traps, filters them, and then forwards the traps to AppManager. For more information, see Working with NetIQ SNMP Trap Receiver.

Prerequisite

To allow this script to access the MIBs for Unified Communications Manager servers, configure your SNMP permissions in AppManager Security Manager *before* using the SNMPTrap_Async script. For more information, see "Configuring SNMP Permissions in Security Manager" on page 1155.

Resource Object

CiscoCM_TrapReceiver

Default Schedule

By default, this script runs on an asynchronous schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Trap Filters	
List of trap OIDs	Type the OIDs (object identifiers) of the traps you want to monitor. You can type one OID or a list of OIDs. If you type a list, separate the OIDs with a comma, like so: `1.3.6.1.2.1.2.2.1.1.1,1.3.6.1.2.1.2.2.1.7.1`

Full path to file with list of trap OIDs	To monitor many OIDs, type the full path to a file that contains a list of the OIDs. Each OID in the file should be on a separate line, like so:
	`1.3.6.1.2.1.2.2.1.1.1`
	`1.3.6.1.2.1.2.2.1.7.1`
	Because the file must be accessible from the AppManager agent, the path must be a local directory on the agent computer or a UNC path.
	Important If you type a UNC path, then the `netiqmc` service must be running as a user that has access to the path.

Event Notification	
Raise trap events?	Select **Yes** to raise an event when a trap message is received from Trap Receiver. The default is Yes.
Event severity when trap is received	Set the severity level, from 1 and 40, to indicate the importance of an event in which a trap is received. The default is 15.

Parameter	How to Set It
Format trap data according to SNMP version	Select the version of SNMP whose formatting should be used for trap event messages. The data provided by each format is the same; only the layout is different. An event message in SNMP v1 format looks like this: An event message in SMMP v2 format looks like this: 
Raise Trap Receiver availability events?	Select **Yes** to raise an event when Trap Receiver becomes unavailable and when Trap Receiver becomes available once again. The default is Yes.
Event severity when Trap Receiver is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes unavailable. The default is 5.
Event severity when Trap Receiver becomes available	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes available after being unavailable. The default is 25.
Data Collection	
Collect data for Trap Receiver availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns a “1” if Trap Receiver is available and a “0” if Trap Receiver is unavailable. The default is unselected.
Interval for collecting Trap Receiver availability data	Specify the frequency with which the script collects Trap Receiver availability data. The default is every 5 minutes.

Working with NetIQ SNMP Trap Receiver

NetIQ SNMP Trap Receiver (Trap Receiver) is installed automatically when you install AppManager for Cisco Unified Communications Manager. Trap Receiver runs as a service, `NetIQTrapReceiver.exe`, and may compete for port usage with any other trap receiver installed on the same computer.

What is NetIQ SNMP Trap Receiver?

At its most basic, a trap receiver is an application that receives traps from SNMP agents. Trap Receiver receives, filters, and forwards SNMP traps to AppManager. When you use Trap Receiver with AppManager for Cisco Unified Communications Manager, the SNMPTrap_Async Knowledge Script raises events when SNMP traps are received.

What is an SNMP Trap?

Simple Network Management Protocol (SNMP) is a protocol-based system used to manage devices on TCP/IP-based networks. From devices on which an SNMP agent resides, such as routers and switches, SNMP sends unsolicited notifications, called traps, to network administrators when thresholds for certain conditions are exceeded. These conditions are defined by the vendor in a device's MIB; the network administrator sets the thresholds.

Traps are composed of Protocol Data Units (PDUs). Each PDU contains the following information, organized in various ways depending on the version of SNMP in use:

- SNMP version number
- Community name of the SNMP agent
- PDU type
- Enterprise OID (object identifier), a unique number that identifies an enterprise and its system objects in the MIB
- IP address of the SNMP agent
- Generic trap type: Cold start, Warm start, Link down, Link up, Authentication failure, and Enterprise
- Specific trap type. When the Generic trap type is set to "Enterprise," a specific trap type is included in the PDU. A specific trap is one that is unique or specific to an enterprise.
- Time the event occurred
- Varbind (variable binding), a sequence of two fields that contain the OID and a value

Understanding Trap Receiver Architecture

Trap Receiver operates on a Client-Server architecture: the *Server*—the stand-alone Trap Receiver application—receives, filters, and forwards SNMP traps to the *Client*—an application that receives traps, such as AppManager. The Server can receive traps on standard UDP port 162 or on any other configured port. The Client and the Server can reside on the same computer or on separate computers.

Communication between Client and Server is implemented as XML messages over a TCP connection. Only one Server is allowed per computer, however, several Clients are allowed per computer. Clients that are registered to the same Server share the same TCP connection. The Server TCP port should be known to all potential Clients.

Understanding the Trap Receiver Configuration File

The configuration file for Trap Receiver, `NetIQTrapReceiver.conf`, identifies the UDP and TCP ports used by Trap Receiver: the UDP port is used for receiving traps; the TCP port is used for communicating with the Client, such as AppManager or another supported NetIQ application. The configuration file also identifies the level of logging you want to use and whether port forwarding is enabled.

By default, the configuration file is installed in `[installation directory]\config`, and has the following format:

```
#################################################################
#
# NetIQTrapReceiver.conf
#
# A configuration file for NetIQ SNMP Trap Receiver
#
#################################################################

#########################
# TCP port
# Syntax: tcp_port [port]
# E.g. : tcp_port 2735
#########################
tcp_port 2735

#########################
# UDP port
# Syntax: udp_port [port]
# E.g. : udp_port 162
#########################
udp_port 162

#########################
# Forwarding
# Syntax: forward [address]:[port] [v1]
# E.g. : forward 127.0.0.1:1000 v1
#########################

#########################
# Log level
# Syntax: log_level error|warning|info|debug|xml
# E.g. : log_level info
#########################
log_level debug
```

If the configuration file cannot be found, cannot be parsed, or does not contain one of the required values, Trap Receiver is initialized with the default configuration as shown above.

When changing values in the configuration file, take into account the following:

- If you change the TCP port number, stop all asynchronous Knowledge Script jobs associated with the modules that support Trap Receiver. Run the Discovery Knowledge Script on all monitored devices to enable the devices to recognize the new TCP port number.
- If you change the UDP port number, also change the UDP port number configured on the devices that send traps to Trap Receiver.
- If another service uses port 2735 or port 162, Trap Receiver *will not start*. The Trap Receiver log file will contain different levels of messages, based on the log_level you choose. Either change the port numbers in the configuration file, stop the service that is using the default Trap Receiver port numbers, or forward the traps coming in to UDP port 162.
- To forward incoming traps to another trap receiver, such as Microsoft SNMP Trap Service, set the Forwarding values as follows:

  ```
  forward [IP address of other trap receiver]:[port number of other trap
  receiver] [SNMP version]
  ```

  For example: `forward 10.40.40.25:167 v1`. By default, incoming traps are not forwarded. For more information, see "Coexisting with Microsoft SNMP Trap Service" on page 1155.
- Restart Trap Receiver after any change to the configuration file. From Control Panel, double-click **Administrative Tools** and then double-click **Services**. Right-click **NetIQ Trap Receiver** and select **Restart**.

Coexisting with Microsoft SNMP Trap Service

Two trap receivers cannot be in use on the same computer while using the same standard UDP port (162). If NetIQ SNMP Trap Receiver and another trap receiver such as Microsoft SNMP Trap Service are installed on the same computer and both are receiving traps, configure Trap Receiver to use the standard UDP port and to forward incoming traps (UDP forwarding) to the other trap receiver. For more information, see "Understanding the Trap Receiver Configuration File" on page 1153.

Then, configure the other trap receiver to use a different, non-standard, UDP port that is not in use by another application. The following are instructions for configuring Microsoft SNMP Trap Service.

To configure Microsoft SNMP Trap Service to use another port:

1. Navigate to `c:\Windows\system32\drivers\etc`.
2. Open the **services** file.
3. In the row for `snmptrap`, change the value for **udp** from 162 to another port number that is not in use by any other application. Use the same port number you set as the forwarding port in the Trap Receiver configuration file.
4. Save and close the **services** file.
5. Restart Windows SNMP Trap Service. In Control Panel, double-click **Administrative Tools** and then double-click **Services**. Right-click **SNMP Trap Service** and select **Restart**.

Tip
To see which ports are in use, run netstat.exe from a command prompt. Then select an available port as the port for the other trap receiver service.

Configuring SNMP Permissions in Security Manager

To allow the SNMPTrap_Async Knowledge Script to access the Management Information Bases (MIBs) for Unified Communications Manager servers, configure your SNMP permissions in AppManager Security Manager *before* using the SNMPTrap_Async script. The SNMP permissions act as a filter for incoming SNMP traps.

The type of information you configure varies according to the version of SNMP that is implemented in your network. AppManager for Cisco Unified Communications Manager supports SNMP versions 1, 2, and 3.

Adding Permissions for SNMP Versions 1 and 2

Configure community string and version information for each Unified Communications Manager server that is monitored by the proxy agent computer. Complete the following fields in the Custom tab of Security Manager.

Field	Description
Label	SNMP

Field	Description
Sub-label	Indicates whether the community string information you are configuring will be used for a single Communications Manager or for all Communications Managers. • *For a single device supported by a particular proxy agent computer*, type the name of the Communications Manager. • *For all devices supported by a particular proxy agent computer*, type `default`.
Value 1	Appropriate read-only community string value, such as `private` or `public`.

Adding Permissions for SNMP Version 3

SNMP trap monitoring in AppManager for Cisco Unified Communications Manager supports the following modes for SNMPv3:

- No authentication; no privacy
- Authentication; no privacy
- Authentication and privacy

In addition, the module supports the following protocols for SNMPv3:

- MD5 (Message-Digest algorithm 5, an authentication protocol)
- SHA (Secure Hash Algorithm, an authentication protocol)
- DES (Data Encryption Standard, encryption protocol)

Your SNMPv3 implementation may support one or more combinations of mode and protocol. That combination dictates the type of information you configure in AppManager Security Manager: user name (or entity), context name, protocol name, and protocol passwords.

Configure community string and version information for each Unified Communications Manager server that is monitored by the proxy agent computer. Complete the following fields in the Custom tab of Security Manager.

Field	Description
Label	`SNMP`
Sub-label	Indicates whether the community string information you are configuring will be used for a single Communications Manager or for all Communications Managers. • *For a single device supported by a particular proxy agent computer*, provide the name of the Communications Manager. • *For all devices supported by a particular proxy agent computer*, type `default`.
Value 1	SNMP user name or entity configured for the device. All SNMPv3 modes require an entry in the **Value 1** field.

Field	Description
Value 2	Name of the context associated with the user name or entity you entered in the **Value 1** field. A context is a collection of SNMP information that is accessible by an entity. If possible, enter a context that provides access to all MIBS for a device. If the device does not support context, type an asterisk (*). All SNMPv3 modes require an entry in the **Value 2** field.
Value 3	Combination of protocol and password appropriate for the SNMPv3 mode you have implemented. • For *no authentication/no privacy mode*, leave the **Value 3** field blank. • For *authentication/no privacy mode*, type `md5` or `sha` and the password for the protocol, separating each entry with a comma. For example, type `md5,abcdefgh` • For *authentication/privacy mode*, type `md5` or `sha` and the associated password, and then type `des` and the associated password, separating each entry with a comma. For example, type `sha,hijklmno,des,nopqrstu`

SystemUpTime

Use this Knowledge Script to monitor the number of hours that the Communications Manager system has been up since the last reboot. This script raises an event if a reboot occurs. In addition, this script generates a data stream for the number of hours that the Communications Manager system has been operational since the last reboot.

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 1172.

Resource Object

CiscoCM_CMServer

Default Schedule

By default, this script runs every five minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SystemUpTime job. The default is 5.
Raise event if system has rebooted?	Select **Yes** to raise an event if Communications Manager has rebooted during the monitoring period. The default is Yes.
Event severity when system has rebooted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Communications Manager has rebooted. The default is 10.
Monitor System Uptime	
Data Collection	
Collect data for system uptime?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of hours that the Communications Manager system has been operational since the last reboot. The default is Yes.

SystemUsage

Use this Knowledge Script to monitor CPU, memory, and disk usage for a Communications Manager server. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following metrics:

- CPU usage (%)
- Physical and virtual memory usage (%)
- Swap space usage (%)
- Active, common, and swap partition usage (%)
- Total processes
- Total threads

This script is a member of the CiscoCM recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 1172.

Resource Object

CiscoCM_CMServer

Default Schedule

By default, this script runs every two minutes.

If you are running this script as part of the Recommended KSG, do not change the schedule. The schedules for the recommended scripts are staggered so as to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SystemUsage job. The default is 5.
Monitor CPU Usage	
Event Notification	
Raise event if CPU usage exceeds threshold?	Select **Yes** to raise an event if CPU usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum CPU usage	Specify the highest percentage of CPU usage that must occur before an event is raised. The default is 90%.
Event severity when CPU usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for CPU usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of CPU usage during the monitoring period. The default is Yes.

Parameter	How to Set It
Monitor Physical Memory Usage	
Event Notification	
Raise event if physical memory usage exceeds threshold?	Select **Yes** to raise an event if physical memory usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum physical memory usage	Specify the highest percentage of physical memory usage that must occur before an event is raised. The default is 80%.
Event severity when physical memory usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which physical memory usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for physical memory usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of physical memory usage during the monitoring period. The default is Yes.
Monitor Virtual Memory Usage	
Event Notification	
Raise event if virtual memory usage exceeds threshold?	Select **Yes** to raise an event if virtual memory usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum virtual memory usage	Specify the highest percentage of virtual memory usage that must occur before an event is raised. The default is 80%.
Event severity when virtual memory usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which virtual memory usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for virtual memory usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of virtual memory usage during the monitoring period. The default is Yes.
Monitor Swap Space Usage	
Event Notification	
Raise event if swap space usage exceeds threshold?	Select **Yes** to raise an event if swap space usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum swap space usage	Specify the highest percentage of swap space that must be in use before an event is raised. The default is 80%.
Event severity when swap space usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which swap space usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for swap space usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of swap space usage during the monitoring period. The default is Yes.
Monitor Active Partition Usage	
Event Notification	
Raise event if active partition usage exceeds threshold?	Select **Yes** to raise an event if active partition usage exceeds the threshold that you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum active partition usage	Specify the highest percentage of active partition usage that must occur before an event is raised. The default is 80%.
Event severity when active partition usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which active partition usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for active partition usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of active partition usage during the monitoring period. The default is Yes.
Monitor Common Partition Usage	
Event Notification	
Raise event if common partition usage exceeds threshold?	Select **Yes** to raise an event if common partition usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum common partition usage	Specify the highest percentage of common partition usage that must occur before an event is raised. The default is 80%.
Event severity when common partition usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which common partition usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for common partition usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of common partition usage during the monitoring period. The default is Yes.
Monitor Swap Partition Usage	
Event Notification	
Raise event if swap partition usage exceeds threshold?	Select **Yes** to raise an event if swap partition usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum swap partition usage	Specify the highest percentage of swap partition usage that must occur before an event is raised. The default is 50%.
Event severity when swap partition usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which swap partition usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for swap partition usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of swap partition usage during the monitoring period. The default is Yes.
Monitor Total Processes	
Event Notification	
Raise event if total processes exceed threshold?	Select **Yes** to raise an event if the number of active processes exceeds the threshold that you set. The default is Yes.
Threshold - Maximum total processes	Specify the highest number of processes that must be active before an event is raised. The default is 250 processes.
Event severity when total processes exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of active processes exceeds the threshold you set. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for total processes?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of processes that are active at each script iteration. The default is Yes.
Monitor Total Threads	
Event Notification	
Raise event if total threads exceed threshold?	Select **Yes** to raise an event if the number of threads exceeds the threshold that you set. The default is Yes.
Threshold - Maximum total threads	Specify the highest number of threads that must be created before an event is raised. The default is 2500 threads.
Event severity when total threads exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of threads exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for total threads?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of threads detected at each script iteration. The default is Yes.

TFTPActivity

Use this Knowledge Script to monitor activity on the Cisco TFTP server. This script raises an event when the number of change notifications for the monitored activity exceeds the threshold that you set. In addition, this script generates data streams for the following metrics:

- Change notifications
- Builds
- Aborted requests
- Not-found requests
- Rejected requests
- Total requests
- Successful requests

Resource Object

CiscoCM_TFTP

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the TFTPActivity job. The default is 5.
Monitor Change Notifications	
Event Notification	
Raise event if change notifications exceed threshold?	Select **Yes** to raise an event if the number of change notifications exceeds the threshold that you set. The default is Yes.
Threshold - Maximum change notifications	Specify the highest number of change notifications that must occur before an event is raised. The default is 10 notifications.
Event severity when change notifications exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of change notifications exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for change notifications?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of change notifications that occurred during the monitoring period.
Monitor Builds	
Event Notification	

Parameter	How to Set It
Raise event if builds exceed threshold?	Select **Yes** to raise an event if the number of builds exceeds the threshold that you set. The default is Yes.
Threshold - Maximum builds	Specify the highest number of builds that must occur before an event is raised. The default is 50 builds.
Event severity when builds exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of builds exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for builds?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of builds that occurred during the monitoring period.
Monitor Aborted Requests	
Event Notification	
Raise event if aborted requests exceed threshold?	Select **Yes** to raise an event if the number of aborted requests exceeds the threshold that you set. The default is Yes.
Threshold - Maximum aborted requests	Specify the highest number of aborted requests that must occur before an event is raised. The default is 0 requests.
Event severity when aborted requests exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of aborted requests exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for aborted requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of aborted requests that occurred during the monitoring period.
Monitor Requests Not Found	
Event Notification	
Raise event if requests not found exceed threshold?	Select **Yes** to raise an event if the number of requests that are not found exceeds the threshold that you set. The default is Yes.
Threshold - Maximum requests not found	Specify the highest number of requests that must be “not found” before an event is raised. The default is 0 requests.
Event severity when requests not found exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of requests that are not found exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for requests not found?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of requests that were not found during the monitoring period.
Monitor Rejected Requests	
Event Notification	
Raise event if rejected requests exceed threshold?	Select **Yes** to raise an event if the number of rejected requests exceeds the threshold that you set. The default is Yes.
Threshold - Maximum rejected requests	Specify the highest number of rejected requests that must occur before an event is raised. The default is 0 requests.
Event severity when rejected requests exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of rejected requests exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for rejected requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of requests that were rejected during the monitoring period.

Parameter	How to Set It
Monitor Total Requests	
Data Collection	
Collect data for total requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of requests, which includes aborted, not-found, rejected, and successful requests.
Monitor Successful Requests	
Data Collection	
Collect data for successful requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of requests that were successful during the monitoring period.

Transcoder_Device

Use this Knowledge Script to monitor the usage of registered transcoder devices. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the number of active resources and for resource usage (%).

Resource Object

CiscoCM_XCode_DeviceObj

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Transcoder_Device job. The default is 5.
Monitor Resource Usage	
Event Notification	
Raise event if resource usage exceeds threshold?	Select **Yes** to raise an event if the percentage of transcoder device usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum resource usage	Specify the highest percentage of transcoder device usage that must occur before an event is raised. The default is 80%.
Event severity when resource usage exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the percentage of transcoder usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for resource usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of transcoder usage at each script iteration.
Monitor Active Resources	
Data Collection	
Collect data for active resources?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of transcoder devices that are active at each script iteration.
Monitor Unavailable Resources	
Event Notification	
Raise event if number of times resources were unavailable exceeds threshold?	Select **Yes** to raise an event if the number of times that transcoder devices were unavailable exceeds the threshold that you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum number of times resources were unavailable	Specify the maximum number of times that transcoder devices can be unavailable before an event is raised. The default is 0 instances.
Event severity number of times resources were unavailable exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of times that transcoder devices were unavailable exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of times resources were unavailable?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of times that transcoder devices were unavailable during the monitoring period.

WebDialer

Use this Knowledge Script to monitor activity for the Cisco Web Dialer application. Web Dialer enables users to place calls from their computers.

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the following monitored activities:

- Failed calls
- Completed calls
- In-progress CTI sessions
- Total CTI sessions
- In-progress HTTP sessions
- Total HTTP sessions

Resource Object

CiscoCM_WebDialer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the WebDialer job. The default is 5.
Monitor Failed Calls	
Event Notification	
Raise event if failed calls exceed threshold?	Select **Yes** to raise an event if the number of failed calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum failed calls	Specify the highest number of calls that must fail before an event is raised. The default is 0 calls.
Event severity when failed calls exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of failed calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for failed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that failed during the monitoring period.
Monitor Completed Calls	
Data Collection	

Parameter	How to Set It
Collect data for completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls that were completed during the monitoring period.
Monitor CTI Sessions in Progress	
Event Notification	
Raise event if CTI sessions in progress exceed threshold?	Select **Yes** to raise an event if the number of CTI sessions in progress exceeds the threshold that you set. The default is Yes.
Threshold - Maximum CTI sessions in progress	Specify the highest number of CTI sessions that must be in progress before an event is raised. The default is 100 sessions.
Event severity when CTI sessions in progress exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of CTI sessions in progress exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for CTI sessions in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of CTI sessions that are in progress at each script iteration.
Monitor CTI Sessions	
Data Collection	
Collect data for CTI sessions?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of CTI sessions that were handled during the monitoring period.
Monitor HTTP Sessions in Progress	
Event Notification	
Raise event if HTTP sessions in progress exceed threshold?	Select **Yes** to raise an event if the number of HTTP sessions in progress exceeds the threshold that you set. The default is Yes.
Threshold - Maximum HTTP sessions in progress	Specify the highest number of HTTP sessions that must be in progress before an event is raised. The default is 100 sessions.
Event severity when HTTP sessions in progress exceed threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of HTTP sessions in progress exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for HTTP sessions in progress?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of HTTP sessions that are in progress at each script iteration.
Monitor HTTP Sessions	
Data Collection	
Collect data for HTTP sessions?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of HTTP sessions that were handled during the monitoring period.

WebPageCheck

Use this Knowledge Script to monitor the availability of and round-trip connection time to the `ccmadmin` and `ccmuser` Web pages. This script raises an event if either Web page is unavailable or if round-trip connection time exceeds the threshold that you set. In addition, this script generates data streams for Web page availability and round-trip time.

If either Web page is unavailable, the detail message records the reason, for example, because the format of the request was invalid or the server name was not found.

This script monitors Web page availability only. To monitor Web page content and usage, use the Knowledge Scripts in a different module: AppManager ResponseTime for Web.

Resource Object

CiscoCM_CMServer

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the WebPageCheck job. The default is 5.
Is Web server secure?	Select **Yes** to indicate that your Communications Manager Web server is a secure Web server (HTTPS). The default is Yes.
Monitor CCMAdmin Web Page Availability	
Event Notification	
Raise event if Web page is unavailable?	Select **Yes** to raise an event if the `ccmadmin` Web page is unavailable. The default is Yes.
Event severity when Web page is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the `ccmadmin` Web page is unavailable. The default is 15.
Data Collection	
Collect data for ccmadmin Web page availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns 100 if the Web page is available and 0 if the Web page is unavailable.
Monitor CCMAdmin Web Page Round-Trip Time	
Event Notification	
Raise event if round-trip time exceeds threshold?	Select **Yes** to raise an event if the round-trip connection time for the `ccmadmin` Web page exceeds the threshold that you set. The default is Yes.
Threshold - Maximum round-trip time	Specify the longest round-trip connection time that can occur before an event is raised. The default is 100 milliseconds.

Parameter	How to Set It
Event severity when round-trip time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which round-trip connection time for the `ccmadmin` Web page exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for round-trip time?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the `ccmadmin` Web page's round-trip connection time during the monitoring period.
Monitor CCMUser Web Page Availability	
Event Notification	
Raise event if Web page is unavailable?	Select **Yes** to raise an event if the `ccmuser` Web page is unavailable. The default is Yes.
Event severity when Web page is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the `ccmuser` Web page is unavailable. The default is 15.
Data Collection	
Collect data for ccmuser Web page availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns 100 if the Web page is available and 0 if the Web page is unavailable.
Monitor CCMUser Web Page Round-Trip Time	
Event Notification	
Raise event if round-trip time exceeds threshold?	Select **Yes** to raise an event if the round-trip connection time for the `ccmuser` Web page exceeds the threshold that you set. The default is Yes.
Threshold - Maximum round-trip time	Specify the longest round-trip connection time that can occur before an event is raised. The default is 100 milliseconds.
Event severity when round-trip time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which round-trip connection time for the `ccmuser` Web page exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for round-trip time?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the round-trip connection time for the `ccmuser` Web page during the monitoring period.

Recommended Knowledge Script Group

The following Knowledge Scripts are members of the CiscoCM recommended Knowledge Script Group (KSG).

- CCM_CallActivity
- CCM_MGCPResources
- CCM_RegisteredResources
- CCM_ResourceAvailability
- CCM_SystemPerformance
- HealthCheck
- RoleStatus
- SystemUpTime
- SystemUsage

The parameters of all scripts in the KSG are set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and run the CiscoCM group on a Unified Communications Manager resource.

Run the KSG on only one cluster at a time. Running the KSG on multiple clusters all at once hinders the proxy agent's ability to spread out processing over time. You can monitor multiple clusters by running the KSG on the first cluster, and then repeating the process for each additional cluster.

The CiscoCM KSG provides a "best practices" usage of AppManager for monitoring your Unified Communications Manager environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView. For more information, see "About Policy-Based Monitoring" in the AppManager Help.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the CiscoCM tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoCM tab are not affected.

When deployed as part of a KSG, a script's default script parameter settings may differ from when the script is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the CiscoCM KSG and want to restore it to its original form, you can reinstall AppManager for Cisco Unified Communications Manager on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\CiscoCM\RECOMMENDED_CiscoCM` directory.

Troubleshooting Missing Data Points

AppManager for Cisco Unified Communications Manager sends consolidated requests to the Unified Communications Manager server to collect the data used by several CiscoCM Knowledge Scripts. AppManager sends these requests 30 seconds before a script begins each iteration. This 30-second data-collection offset allows enough time for AppManager to execute the query before a script requires the data.

If you notice data points are missing from a job's data stream, it may be that 30 seconds is not enough time for AppManager to execute all of the queries you need, most likely because you are running several scripts on the same schedule.

You can increase the data-collection offset time by changing a Registry setting:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0\NetIQmc\DataRecorder\Collection
Offset
```

In the right pane of the Registry Editor, double-click **CiscoCM** and change the **Decimal** value from 30 seconds to a larger value that will allow enough time for AppManager to execute the queries for all of the scripts you are running. Keep the value *less* than the shortest interval specified by any Knowledge Script. For example, if one script runs every one minute, but the others run every five minutes, do not change the Registry setting to a value equal to or greater than 60 seconds.

Changes to this Registry setting affect the data-collection offset time for the following Knowledge Scripts:

AnalogAccess_GatewayUsage	Annunciator_Device	AttendantConsole
CCM_CallActivity	CCM_MediaResources	CCM_MGCPResources
CCM_RegisteredResources	CCM_ResourceAvailability	CCM_SystemPerformance
CFB_Hardware_Device	CFB_Software_Device	CFB_Video_Device
CTIManager	ExtensionMobility	GatekeeperActivity
GeneralCounter	H323_Gateway_CallActivity	H323_Trunk_CallActivity
HuntAndRouteList	Locations	MediaStreamingApp
MGCP_FXO_CallActivity	MGCP_FXS_CallActivity	MGCP_GatewayUsage
MGCP_PRI_CallActivity	MGCP_PRI_ChannelHealth	MGCP_T1CAS_CallActivity
MGCP_T1CAS_ChannelHealth	MOH_Device	MTP_Device
SIP_Trunk_CallActivity	SystemUpTime	SystemUsage
TFTPActivity	Transcoder_Device	WebDialer

Chapter 20
CiscoCME Knowledge Scripts

The CiscoCME category provides the following Knowledge Scripts for monitoring Cisco CallManager Express resources.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
Device_Reset	Resets CallManager Express IP phones for reasons such as troubleshooting or picking up new default firmware.
Device_Status	Monitors the status of key CallManager Express devices.
Extension_Check	Monitors for duplicate phone extension numbers. This script looks for all phones configured in CallManager Express, regardless of whether they are registered.
Phone_Inventory	Generates an inventory of the phone details for phones attached to CallManager Express.
Set_Key_Phones	Designates one or more "key" phones. After you designate key phones, you then can choose to monitor only key phones.
SRST_Failover	Monitors a device operating in SRST (Survivable Remote Site Telephony) mode for registered phones or network connectivity failure, which indicate a failover from CallManager.

Device_Reset

Use this Knowledge Script to reset or restart CallManager Express IP phones for reasons such as troubleshooting or picking up new default firmware. Use this script in conjunction with Device_Status to ensure selected phones have upgraded successfully.

Notes

- Only an AppManager administrator may run this script.
- The AXL API does not return a failure if you try to reset an unregistered phone, or if you try to reset a phone with an invalid or incorrect name, or if you try to reset a phone that has never been registered with the router. Therefore, AppManager has no way of knowing the reset did not succeed.

Resource Object

CiscoCME

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following values as needed:

Parameter	How To Set It
Event Notification	
Raise event if reset/restart succeeds?	Set to **Yes** to raise an event if the device was successfully reset or restarted. The default is Yes.
Event severity when reset/restart succeeds	Set the severity level of the event, from 1 to 40, to indicate the importance of a successful event. The default is 25.
Event severity when reset/restart error occurs	Set the severity level of the event, from 1 to 40, to indicate the importance of an event in which errors occurred. The default is 5.
Options	
Function type	Choose **Reset** to shut down a registered device and then bring it back up. Choose **Restart** to restart a registered device without first shutting it down. The default is Reset.
Device selection type	Select the type of device you want to reset or restart. All devices of that type will be reset or restarted. • Select **DeviceName** to reset or restart a specific device or devices. If you select this type, you must type a device name or list of name in the *Device name list* parameter, or identify the location of a list of devices in *Full path to file with list of devices*. • Select **All** to reset or restart all phones at once. • Select **AllSequenced** to reset/restart phones in sequential order. **Note** The **All** and **AllSequenced** actions may take a long time to complete.

Parameter	How To Set It
Device name list	Use this parameter if you selected **DeviceName** in the *Device selection type* parameter. Type the name of the device you want to reset or restart. You can also type a list of device names, separated by a comma. For example: `SEP999999994000,SEP999999994001`. **Note** If you type a device name, ignore the *Full path to file with list of devices* parameter.
Full path to file with list of devices	Use this parameter if you selected **DeviceName** in the *Device selection type* parameter. Type the full path to a file on the agent computer containing a list of the devices you want to restart or reset. The file should contain the device names on one or more lines. If you specify the criteria on one line, separate each item with a comma. For example: `SEP999999994000,SEP999999994001`. If you specify the criteria on multiple lines, ensure each line contains only one entry. For example: • SEP999999994002 • SEP999999994000 • SEP999999994004 **Note** If you type a file path, ignore the *Device name list* parameter.

Device_Status

Use this Knowledge Script to monitor the status of key CallManager Express devices. The possible statuses are:

- **Registered**. This status indicates the device is available.
- **Unregistered**. This status indicates a device previously registered with CallManager Express has become unregistered. This status may be generated as part of a normal unregistration event, or can be due to another reason such as loss of keepalives.
- **Deceased**. This status indicates the device has not been registered to CallManager Express for a long time, or the device was added to CallManager Express but never registered.

Note
Phones of model type 7905G are designated in event messages as an "Others" type. (Cisco issue CSCee28952)

The first time you run this script, it builds a device list from the criteria you have selected. At each subsequent interval, the script checks the status of these devices. If the number or percentage of these devices that are registered does not meet the threshold you set, an event is raised.

Resource Object

CiscoCME

Default Schedule

By default, this script runs every one minute.

Setting Parameter Values

Set the following values as needed:

Parameter	How To Set It
Event Notification	
Raise event if key devices fall below threshold?	Set to **Yes** to raise an event if the number or percentage of registered key devices falls below the threshold you set. The default is Yes. The detailed message for an event contains the following information about each device that is not registered: • Device Name • Directory number(s) • IP address (if available) • Status • CallManager Express address where device was registered (if available) • Model
Event severity when key devices fall below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number or percentage of key devices fell below the threshold. The default is 10.

Parameter	How To Set It
Raise event if key devices cross threshold and then return?	Set to **Yes** to raise an event if the number or percentage of key devices falls below the minimum, but is now within an acceptable range. The default is Yes. The detailed message for the event will contain the percentage of registered devices and the threshold percentage.
Event severity when key devices cross threshold and then return	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number or percentage of key devices fell below the minimum, but is now within an acceptable range. The default is 20.
Raise initial event with current status?	Set to **Yes** to raise an informational event that contains the current status of selected devices. The default is Yes. This event is raised only upon the first run of this script. The event message returns the following details about each device: • Device Name • Directory number(s) • IP address (if available) • Status • CallManager Express address where device was registered (if available) • Model
Format status event in XML?	Set to **Yes** to format the informational event containing the current status in XML. The default is Yes. If you use XML for the event, it will not be sent to any Actions defined for the script. If you want this information sent to an Action, do not check this checkbox. The detailed message will then be formatted in .csv format.
Event severity for initial event with current status	Set the severity level, from 1 to 40, to indicate the importance of the informational event. The default is 30.
Data Collection	
Collect data?	Set to **Yes** to collect data for graphs and charts. If enabled, data collection returns the number of devices being monitored and the number of those devices that are registered. The default is unchecked.
Monitoring	
Select by type	Choose the type of the selection criteria to be used to get the list of devices to monitor. Note, some criteria may not make sense for every device type. Valid values are: • DeviceName, which is the default • KeyPhones
Selection criteria	Type the selection criteria for the devices to be monitored. You can specify the actual item or you can specify a pattern by using the * wildcard. For example, to monitor all devices with device names that begin with SEP, type `SEP*`. The wildcard works only at the end of a string. To monitor all devices, accept the default of *. You can type multiple items by separating each item with a comma. For example: `SEP0009A*,SEP0009B*` . **Note** If you type a file path in *Full path to file with list of selection criteria*, ignore this parameter.

Parameter	How To Set It
Full path to file with selection criteria	Type the full path to a file on the agent computer containing a list of the selection criteria. The file should contain the selection criteria on one or more lines. You can specify the actual item or you can specify a pattern by using the * wildcard. If you specify the criteria on one line, separate each item with a comma. For example: `SEP0009A*,SEP0009B*`. If you specify the criteria on multiple lines, ensure each line contains only one entry. For example: • SEP0009A* • SEP999999994000 • SEP00044* **Note** If you type a file path, ignore the *Selection criteria* parameter.
Threshold type	Select whether you want to monitor for a **Percentage** threshold or a **Number** threshold. The default is percentage.
Threshold - Minimum % devices registered	Specify the minimum percentage of devices that must have a status of "Registered" before an event is raised. The default is 75%.
Threshold - Minimum # devices registered	Specify the minimum number of devices that must have a status of "Registered" before an event is raised. The default is 0.

Extension_Check

Use this Knowledge Script to monitor for duplicate phone extension numbers. This script will look for all phones configured in CallManager Express, regardless of whether they are registered. This script automatically raises an event if duplicate extension numbers are discovered.

Resource Object

CiscoCME

Default Schedule

By default, this script runs every four hours.

Setting Parameter Values

Set the following values as needed:

Parameter	How To Set It
Event Notification	
Raise event if no duplicate extensions found?	Set to **Yes** to create an event if no duplicate extension numbers are discovered. The default is Yes.
Event severity when no duplicate extensions found	Set the severity level, from 1 to 40, to indicate the importance of an event in which no duplicates are found. The default is 25.
Event severity when duplicate extensions found	Set the severity level, from 1 to 40, to indicate the importance of an event in which duplicates are found. The default is 10.

Phone_Inventory

Use this Knowledge Script to create an inventory of phone details for phones attached to CallManager Express.

Note
Phones of model type 7905G are designated in event messages as an "Others" type. (Cisco issue CSCee28952)

Resource Object

CiscoCME

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following values as needed:

Parameter	How To Set It
Event Notification	
Raise informational event when inventory completes?	Set to **Yes** to raise an event when the inventory is complete. The event message contains the phone inventory details. The default is Yes.
Event severity when informational event is raised	Set the severity level of the event, from 1 to 40, to indicate the importance an informational event. The default is 25.
Event severity when no phones are found	Set the severity level of the event, from 1 to 40, to indicate the importance of an event in which no phones are found. The default is 30.
Event severity when inventory fails	Set the severity level of the event, from 1 to 40, to indicate the importance of an event in which the inventory fails. The default is 15.
Selection Options	
Select by	Choose the type of the selection criteria you want to use to create the list of phones. Valid values are: • Name, which is the default • KeyPhones
Selection criteria	Type the selection criteria for the devices to be monitored. You can specify the actual item or you can specify a pattern by using the * wildcard. For example, to monitor all devices with device names that begin with SEP, type `SEP*`. The wildcard works only at the end of a string. To monitor all devices, accept the default of *. You can type multiple items by separating each item with a comma. For example: `SEP0009A*,SEP0009B*`. **Note** If you type selection criteria, then ignore the *Full path to file with selection criteria* parameter.

Parameter	How To Set It
Full path to file with selection criteria	Type the full path to a file on the agent computer containing a list of the selection criteria. The file should contain the selection criteria on one or more lines. You can specify the actual item or you can specify a pattern by using the * wildcard. If you specify the criteria on one line, separate each item with a comma. For example: `SEP0009A*,SEP0009B*`. If you specify the criteria on multiple lines, ensure each line contains only one entry. For example: • SEP0009A* • SEP999999994000 • SEP00044* **Note** If you type a file path, ignore the *Selection criteria* parameter.
Result File Options	
Write details to result file?	Set to **Yes** to output the inventory results to a .csv file. The default is Yes.
Result file name	Type the full path or a UNC path to a location on the agent computer where the inventory result file should be written. The default location is `c:\Program Files\NetIQ\Temp\NetIQ_Debug\PhoneInventory`. The following details are returned about each phone: • Name • Directory number(s) • Model • IP address (if available) • CallManager Express where device is\was registered (if available) • Status • Status Time **Note** The Phone_Inventory script can be run against multiple CMEs at one time. To avoid confusion, the name of the CME device is added to the name of the output file. The inventory results for each CME are output to a separate file, identified by the CME name.
Overwrite existing file?	Set to **Yes** to overwrite the existing file. Uncheck Yes to add any new results to the existing file. The default is unchecked. **Warning** Deselecting Yes and then running the script many times could result in the creation of a very large file.
List only phone with status of	Use this parameter to limit the phones listed in the results file to only those whose status is one of the following: • Any, which is the default • Not Registered • Registered • Unregistered • Deceased **Note** Setting this parameter to a value of **Not Registered** will list those phones with a status of Unregistered or Deceased.
Order by	Accept the default of **Name** to display the contents of the results file in order by the phone name. Select **DirectoryNumber** to display the contents of the results file in order by directory number.

Set_Key_Phones

Use this Knowledge Script to designate one or more phones as “key” phones. The “key phone” feature of CallManager Express allows you to specify certain phones to be used for monitoring or management purposes. For example, you may not want to monitor all phones at a particular location, but instead monitor only a select subset of important, or key, phones.

The AXL API identifies which phones are key and which are not.

Notes

- This script does not support a device operating in SRST (Survivable Remote Site Telephony) mode. Devices go into SRST mode when the WAN link to the Cisco CallManager at the central site goes down, or when the connection to the CallManager is lost.
- You cannot designate an ATA186 device as a key phone. (Cisco issue CSCee28929)

Resource Object

CiscoCME

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following values as needed:

Parameter	How To Set It
Event Notification	
Raise event if key designation succeeds?	Set to **Yes** to generate an event when key phones are successfully designated. The default is Yes.
Event severity when key designation succeeds	Set the severity level of the event, from 1 to 40, to indicate the importance of an event in which key phones are successfully designated. The default is 25.
Event severity when key designation fails	Set the severity level of the event, from 1 to 40, to indicate the importance of the event in which the key designation attempt fails. The default is 5.
Set Options	

Parameter	How To Set It
List of phones	Use this parameter to specify the names of phones you want to designate as key phones. You must specify at least one phone. You can type multiple names by separating them with a comma. For example: `SEP999999994002,SEP999999994007`. **Note** If you type a list of phones, ignore the *Full path to file with list of phones* parameter.
Full path to file with list of phones	Type the full path to a file on the agent computer containing a list of the names of key phones. The file should contain the names on one or more lines. If you specify the key phones on one line, separate each item with a comma. For example: `SEP999999994000,SEP999999994001`. If you specify the phones on multiple lines, ensure each line contains only one entry. For example: • SEP999999994002 • SEP999999994000 • SEP999999994004 **Note** If you type a full path, ignore the *List of phones* parameter.

SRST_Failover

Use this Knowledge Script to monitor for registered phones or connectivity failure to the SRST (Survivable Remote Site Telephony) device, which indicate a failover has occurred. A device operating in SRST mode can be monitored for SRST failover. Failover occurs when the WAN link to the CallManager at the central site goes down, or when the connection to the CallManager is lost.

This script raises events that identify registered phones and connectivity failures.

Note
This script cannot be used on a router operating in CME mode.

Resource Object

CiscoCME

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following values as needed:

Parameter	How To Set It
Event Notification	
Raise event when phones register with SRST?	Set to **Yes** to raise an event when phones register with SRST, indicating failover. The default is Yes.
Event severity when phones register with SRST	Set the severity level, from 1 to 40, to indicate the importance of an event in which phones register with SRST. The default is 10.
Raise event when connectivity fails?	Set to **Yes** to raise an event when connectivity failure occurs. The default is Yes.
Event severity when connectivity fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which connectivity fails. The default is 10.

Chapter 21
CiscoICD Knowledge Scripts

AppManager for Cisco Integrated Contact Distribution provides the following Knowledge Scripts for monitoring a Cisco Unified Contact Center Express (UCCX) environment. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AgentsLoggedOn	Determines how many licensed (active) agents are logged on and ready for work.
CallStatistics	Monitors the number of incoming and outgoing calls that are being accepted or generated.
CSQ_ServiceLevel	Monitors handled calls, caller wait time, and percentage of calls that met the service level agreement (SLA) for a contact service queue.
ICD_CpuHigh	Monitors CPU utilization for each monitored Cisco UCCX service.
ICD_EventLog	Monitors the CPU resources that UCCX services are consuming.
ICD_HealthCheck	Monitors the status of Cisco UCCX services and to restart any selected service that is down.
ICD_MemoryHigh	Monitors memory pool usage and total memory usage for each monitored Cisco UCCX service.
ICD_RestartService	Schedules a Cisco UCCX service to stop and then restart after a specified time interval.
ICD_SystemUsage	Monitors the amount of CPU and memory that UCCX is using.
IIS_CpuHigh	Monitors CPU usage for IIS application processes.
IIS_HealthCheck	Checks IIS servers, Web site status, and the queue length for blocked I/O requests.
IIS_KillTopCPUProcs	Monitors the CPU usage for the IIS dllhost and mtx processes.
IIS_MemoryHigh	Detects whether an IIS application process has exceeded the memory usage threshold you set.
IIS_ServiceUpTime	Monitors the uptime for Web sites and services.
SQL_Accessibility	Monitors whether the SQL Server database is accessible.
SQL_CPUUtil	Monitors CPU usage by SQL Server processes.
SQL_DataGrowthRate	Monitors data growth and shrink rates for all SQL Server databases.
SQL_DBGrowthRate	Monitors database growth and shrink rates.
SQL_MemUtil	Monitors memory usage by SQL Server processes.

Knowledge Script	What It Does
SQL_RestartServer	Restarts a SQL server.
Recommended Knowledge Script Group	Performs essential monitoring of your Cisco UCCX environment.

AgentsLoggedOn

Use this Knowledge Script to determine how many licensed (active) agents are logged on and ready for work. This script raises an event if a monitored value exceeds or falls below a threshold. In addition, this script can generate data streams for total number of agents and number of agents logged on.

Resource Object

Agent child object under the CiscoICD parent object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if logged-on agents exceed the threshold?	Select **Yes** to raise an event if the percentage of logged-on agents exceeds the maximum threshold you set. The default is Yes.
Severity when logged-on agents exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of logged-on agents exceeds the maximum threshold you set. The default is 15.
Raise event if logged-on agents fall below the threshold	Select **Yes** to raise an event when the percentage of logged-on agents is less than the minimum threshold you set. The default is Yes.
Severity when logged-on agents fall below the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of logged-on agents is less than the minimum threshold you set. The default is 15.
Data Collection	
Collect data?	Select **Yes** to collect data for charts and graphs. The default is unselected. This script generates two data streams: • Total number of agents • Number of agents logged on
Monitoring	
Threshold - Maximum agents logged on	Specify the highest percentage of agents that can be logged on before an event is raised. The default is 100%.
Threshold - Minimum agents logged on	Specify the lowest percentage of agents that can be logged on before an event is raised. The default is 1%.
SQL username	Specify the database user login account you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. **Note** If a SQL username is required, configure the username into AppManager Security Manager.

CallStatistics

Use this Knowledge Script to monitor the following call statistics for a UCCX server:

- Incoming calls - the number of calls coming in to the UCCX system
- Outgoing calls - the number of calls going out of the UCCX system
- Internal calls - the number of calls made within the UCCX system
- Redirect in calls - the number of incoming calls that are automatically redirected to an appropriate agent or other destination
- Transfer in calls - the number of calls transferred in to the UCCX system
- Preview outbound calls - the number of calls for which an agent reviewed lead history before dialing
- Average call duration - the average length of incoming and outgoing calls

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for all monitored statistics.

Resource Object

CiscoICD parent object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if incoming calls exceed the threshold?	Select **Yes** to raise an event if the number of incoming calls exceeds the threshold you set. The default is Yes.
Event severity when incoming calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of incoming calls exceeds the threshold you set. The default is 15.
Raise event if outgoing calls exceed the threshold?	Select **Yes** to raise an event if the number of outgoing calls exceeds the threshold you set. The default is Yes.
Event severity when outgoing calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of outgoing calls exceeds the threshold you set. The default is 15.
Raise event if internal calls exceed the threshold?	Select **Yes** to raise an event if the number of internal calls exceeds the threshold you set. The default is Yes.
Event severity when internal calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of internal calls exceeds the threshold you set. The default is 15.

Parameter	How To Set It
Raise event if redirect in calls exceed the threshold?	Select **Yes** to raise an event if the number of redirected incoming calls exceeds the threshold you set. The default is Yes.
Event severity when redirect in calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of redirected incoming calls exceeds the threshold you set. The default is 15.
Raise event if transfer in calls exceed the threshold?	Select **Yes** to raise an event if the number of transferred incoming calls exceeds the threshold you set. The default is Yes.
Event severity when transfer in calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of transferred incoming calls exceeds the threshold you set. The default is 15.
Raise event if preview outbound calls exceed the threshold?	Select **Yes** to raise an event if the number of preview outbound calls exceeds the threshold you set. The default is Yes.
Event severity when preview outbound calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of preview outbound calls exceeds the threshold you set. The default is 15.
Raise event if call duration exceeds the threshold?	Select **Yes** to raise an event if the duration of calls exceeds the threshold you set. The default is Yes.
Event severity when call duration exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the duration of calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for incoming calls?	Select **Yes** to collect data for charts and graphs. When enabled, data collection returns the number of incoming calls for the monitoring interval. The default is unselected.
Collect data for outgoing calls?	Select **Yes** to collect data for charts and graphs. When enabled, data collection returns the number of outgoing calls for the monitoring interval. The default is unselected.
Collect data for internal calls?	Select **Yes** to collect data for charts and graphs. When enabled, data collection returns the number of internal calls for the monitoring interval. The default is unselected.
Collect data for redirect in calls?	Select **Yes** to collect data for charts and graphs. When enabled, data collection returns the number of redirected incoming calls for the monitoring interval. The default is unselected.
Collect data for transfer in calls?	Select **Yes** to collect data for charts and graphs. When enabled, data collection returns the number of transferred incoming calls for the monitoring interval. The default is unselected.
Collect data for preview outbound calls?	Select **Yes** to collect data for charts and graphs. When enabled, data collection returns the number of preview outbound calls for the monitoring interval. The default is unselected.
Collect data for call duration?	Select **Yes** to collect data for charts and graphs. When enabled, data collection returns the average length of incoming and outgoing calls for the monitoring interval. The default is unselected.
Monitoring	
Threshold - Maximum incoming calls	Specify the highest number of incoming calls that can be received before an event is raised. The default is 100 calls.

Parameter	How To Set It
Threshold - Maximum outgoing calls	Specify the highest number of outgoing calls that can be made before an event is raised. The default is 100 calls.
Threshold - Maximum internal calls	Specify the highest number of internal calls that can be made before an event is raised. The default is 100 calls.
Threshold - Maximum redirect in calls	Specify the highest number of incoming calls that can be redirected before an event is raised. The default is 100 calls.
Threshold - Maximum transfer in calls	Specify the highest number of incoming calls that can be transferred before an event is raised. The default is 100 calls.
Threshold - Maximum preview outbound calls	Specify the highest number of preview outbound calls that can be made before an event is raised. The default is 100 calls.
Threshold - Maximum call duration	Specify the longest duration for incoming and outgoing calls that can occur before an event is raised. The default is 5 minutes.
SQL username	Enter the database user login account you want to use to access the UCCX SQL Server database. You can use the sa account or other user login account that has been configured on the agent computer. Leave this parameter blank in order to use Windows authentication. **Note** If a SQL username is required, configure the username into AppManager Security Manager.

CSQ_ServiceLevel

Use this Knowledge Script to monitor handled calls, caller wait time, and percentage of calls that do not meet the service level agreement (SLA) for the Contact Service queue. This script raises an event if a threshold is exceeded. In addition, this script can generate data streams for the number of handled calls, the total amount of caller wait time, and the number of calls not meeting SLA.

Resource Object

Cisco ICD Contact Service queue object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if handled calls exceed the threshold?	Select **Yes** to raise an event if the number of handled calls exceeds the threshold you set. The default is Yes.
Event severity when handled calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of handled calls exceeds the threshold you set. The default is 15.
Raise event if caller wait time exceeds the threshold?	Select **Yes** to raise an event if the caller wait time exceeds the threshold you set. The default is Yes.
Event severity when caller wait time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the amount of caller wait time exceeds the threshold you set. The default is 15.
Raise event if calls not meeting the SLA exceed the threshold?	Select **Yes** to raise an event when the percentage of calls not meeting the SLA exceeds the threshold you set. The default is Yes.
Event severity when calls not meeting SLA exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that do not meet the SLA exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for handled calls?	Select **Yes** to collect data for charts and graphs. When enabled, data collection returns the number of calls that were handled during the monitoring interval. The default is unselected.
Collect data for caller wait time?	Select **Yes** to collect data for charts and graphs. When enabled, data collection returns the average amount of time that callers waited during the monitoring interval. The default is unselected.
Collect data for calls not meeting the SLA?	Select **Yes** to collect data for charts and graphs. When enabled, data collection returns the percentage of calls that did not meed the SLA during the monitoring interval. The default is unselected.
Monitoring	
Threshold - Maximum handled calls	Specify the highest number calls that can be handled before an event is raised. The default is 20 calls.

Parameter	How To Set It
Threshold - Maximum caller wait time	Specify the longest amount of time a caller can wait before an event is raised. The default is 5 minutes.
Threshold - Maximum calls not meeting SLA	Enter the highest percentage of calls-not-meeting-the-SLA that can occur before an event is raised. The default is 5%.
SQL username	Enter the database user login account you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. **Note** If a SQL username is required, configure the username into AppManager Security Manager.

ICD_CpuHigh

Use this Knowledge Script to monitor the CPU resources that UCCX services are consuming. This script raises an event if a service's CPU utilization exceeds the thresholds you set. The script monitors CPU usage for each service individually and the total CPU usage for all services. If a process is not found, the script assumes the process is not running, and reports zero as the CPU result.

Resource Object

Service child object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if CPU usage exceeds the threshold?	Select **Yes** to raise an event if the CPU usage of any monitored service exceeds the threshold you set. The default is Yes.
Event severity when CPU usage exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CPU usage of any monitored service exceeds the threshold you set. The default is 10.
Data Collection	
Collect data?	Select **Yes** to collect data about CPU usage for graphs and reports.When enabled, data collection returns the percentage of CPU monitored services consumed during the monitoring interval. The default is unselected.
Monitoring	
Version 3.x Services	
Monitor Cisco CRA Engine?	Select **Yes** to monitor CPU usage for the Cisco CRA Engine. The default is Yes.
Threshold: Maximum Cisco CRA Engine CPU usage	Specify the highest percentage of CPU that the CRA Engine can use before an event is raised. The default is 80%.
Monitor Cisco AVVID Alarm?	Select **Yes** to monitor CPU usage for the Cisco AVVID Alarm. The default is Yes.
Threshold: Maximum Cisco AVVID Alarm CPU usage	Specify the highest percentage of CPU that the AVVID Alarm can use before an event is raised. The default is 20%.
Monitor Cisco Purging Scheduler?	Select **Yes** to monitor CPU usage for the Cisco Purging Scheduler. The default is Yes.
Threshold: Maximum Cisco Purging Scheduler CPU usage	Specify the highest percentage of CPU that the Purging Scheduler can use before an event is raised. The default is 20%.
Monitor Cisco CRA Servlet Engine?	Select **Yes** to monitor CPU usage for the Cisco CRA Servlet Engine. The default is Yes.

Parameter	How To Set It
Threshold: Maximum Cisco CRA Servlet Engine CPU usage	Specify the highest percentage of CPU that the CRA Servlet Engine can use before an event is raised. The default is 20%.
Monitor Cisco Desktop Enterprise Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop Enterprise Service. The default is Yes.
Threshold: Maximum Cisco Desktop Enterprise Service CPU usage	Specify the highest percentage of CPU that the Desktop Enterprise Service can use before an event is raised. The default is 20%.
Monitor Cisco Desktop RASCAL Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop RASCAL Service. The default is Yes.
Threshold: Maximum Cisco Desktop RASCAL Service CPU usage	Specify the highest percentage of CPU that the Desktop RASCAL Service can use before an event is raised. The default is 20%.
Monitor Cisco Desktop Sync Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop Sync Service. The default is Yes.
Threshold: Maximum Cisco Desktop Sync Service CPU usage	Specify the highest percentage of CPU that the Desktop Sync Service can use before an event is raised. The default is 20%.
Monitor Cisco Desktop TAI Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop TAI Service. The default is Yes.
Threshold: Maximum Cisco Desktop TAI Service CPU usage	Specify the highest percentage of CPU that the Desktop TAI Service can use before an event is raised. The default is 20%.
Monitor Cisco Desktop VoIP Monitor Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop VoIP Monitor Service. The default is Yes.
Threshold: Maximum Cisco Desktop VoIP Monitor Service CPU usage	Specify the highest percentage of CPU that the Desktop VoIP Monitor Service can use before an event is raised. The default is 20%.
Version 4.x Services	
Monitor Cisco CRS Node Manager?	Select **Yes** to monitor CPU usage for the Cisco CRS Node Manager. The default is Yes.
Threshold: Maximum Cisco CRS Node Manager CPU usage	Specify the highest percentage of CPU that the CRS Node Manager can use before an event is raised. The default is 80%.
Monitor Cisco AVVID Alarm?	Select **Yes** to monitor CPU usage for the Cisco AVVID Alarm. The default is Yes.
Threshold: Maximum Cisco AVVID Alarm CPU usage	Specify the highest percentage of CPU that the AVVID Alarm can use before an event is raised. The default is 20%.
Monitor Cisco Desktop Enterprise Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop Enterprise Service. The default is Yes.
Threshold: Maximum Cisco Desktop Enterprise Service CPU usage	Specify the highest percentage of CPU that the Desktop Enterprise Service can use before an event is raised. The default is 20%.
Monitor Cisco Desktop IP Phone Agent Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop IP Phone Agent Service. The default is Yes.
Threshold: Maximum Cisco Desktop IP Phone Agent Service CPU usage	Specify the highest percentage of CPU that the Desktop IP Phone Agent Service can use before an event is raised. The default is 20%.

Parameter	How To Set It
Monitor Cisco Desktop LDAP Monitor Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop LDAP Monitor Service. The default is Yes.
Threshold: Maximum Cisco Desktop LDAP Monitor Service CPU usage	Specify the highest percentage of CPU that the Desktop LDAP Monitor Service can use before an event is raised. The default is 20%.
Monitor Cisco Desktop License and Resource Manager Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop License and Resource Manager Service. The default is Yes.
Threshold: Maximum Cisco Desktop License and Resource Manager Service CPU usage	Specify the highest percentage of CPU that the Desktop License and Resource Manager Service can use before an event is raised. The default is 20%.
Monitor Cisco Desktop Recording and Statistics Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop Recording and Statistics Service. The default is Yes.
Threshold: Maximum Cisco Desktop Recording and Statistics Service CPU usage	Specify the highest percentage of CPU that the Desktop Recording and Statistics Service can use before an event is raised. The default is 20%.
Monitor Cisco Desktop Recording Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop Recording Service. The default is Yes.
Threshold: Maximum Cisco Desktop Recording Service CPU usage	Specify the highest percentage of CPU that the Desktop Recording Service can use before an event is raised. The default is 20%.
Monitor Cisco Desktop Sync Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop Sync Service. The default is Yes.
Threshold: Maximum Cisco Desktop Sync Service CPU usage	Specify the highest percentage of CPU that the Desktop Sync Service can use before an event is raised. The default is 20%.
Monitor Cisco Desktop VoIP Monitor Service?	Select **Yes** to monitor CPU usage for the Cisco Desktop VoIP Monitor Service. The default is Yes.
Threshold: Maximum Cisco Desktop VoIP Monitor Service CPU usage	Specify the highest percentage of CPU that the Desktop VoIP Monitor Service can use before an event is raised. The default is 20%.

ICD_EventLog

Use this Knowledge Script to monitor Windows event log entries from Cisco UCCX during the past *n* hours. This script raises an event if log entries are detected. In addition, this script generates data streams for entries from different log files.

Resource Object

CiscoICD parent object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event for log entries?	Select **y** to raise an event when the log contains entries that match your filtering criteria. The default is y.
Collect data?	Select **y** to collect data about log entries for charts and graphs. When enabled, data collection returns the number of entries placed in different log files during the monitoring interval. The default is n.
Separate data?	Select **y** to separate events entries from different log files into different data streams. If n selected, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. The default is n. For example, if you are monitoring both the System and Application logs, you can set this parameter to **y** so that events in the System log are tracked separately from events in the Application log.
Log source	Specify the event log you want to monitor. You can specify multiple event logs, separated by commas. For example: `System,Application`. The default is Application.
Type: Error	Select **y** to monitor for error events. If n is selected, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is y.
Type: Warning	Select **y** to monitor for warning events. If n is selected, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is y.
Type: Information	Select **y** to monitor for information events. If n is selected, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is n.
Type: Success Audit	Select **y** to monitor for success audit events. If n is selected, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is n.
Type: Failure Audit	Select **y** to monitor for failure audit events. If n is selected, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is n.

Parameter	How To Set It
Instructions for filters: To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log. The search string can contain criteria used to include entries, exclude entries, or both.· • Separate include and exclude criteria with a colon (:). For example, `net:logon`. • Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ`. • If you are specifying only include criteria, the colon is not necessary. For example, `SQL`. • If you are specifying only exclude criteria, start the search string with a colon. For example, `:defragmentation,cleanup`.	
Event source filter	Specify the names of event sources to look for, separating multiple names with commas. For example: `NTDS KCC,NTDS General`
Event category filter	Specify the names of event categories to look for, separating multiple names with commas.
Event ID filter	Specify a single event ID or a range of event IDs, separating multiple entries with commas. For example: `1094,1404-1463`
Event user filter	Specify user names to look for, separating multiple entries with commas. For example: `Pat,Chris,Alex`
Computer filter	Specify a single or multiple computer names to look for; separate multiple entries by commas. For example: `SHASTA,MARS`
Event description filter	Specify keywords or phrases to look for in event descriptions. The string can contain spaces, underscores, and periods. Separate multiple entries with commas. For example: `data loss during system failures,corrupt indices,Inter-Site Transport objects failed`
Maximum number of entries per event report	Specify the maximum number of Windows log entries that can be returned in each event report. For example, if this value is set to 30 and 67 log entries are found, three reports are created: two reports containing 30 entries and one report containing seven entries. The default is 30. The Message column on the Events tab in the Operator Console displays the number of entries in each report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.
Event severity for log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event. You may want to adjust the severity depending on the types of events for which you are checking. The default is 15.

ICD_HealthCheck

Use this Knowledge Script to monitor the status of Cisco UCCX services and to restart any selected service that is down. This script raises an event if a service is not running, if a service does not restart automatically, if a service successfully restarts, if a service has been set to not restart, or if a selected service does not exist.

Resource Object

Contact Service Queue child object

Default Schedule

By default, this script runs every one minute.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if service is not running?	Select **Yes** to raise an event if a monitored services is not running. The default is Yes.
Event severity when service is not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which a monitored service is not running. The default is 15.
Raise event if service auto-start fails?	Select **Yes** to raise an event when a monitored service fails to restart. The default is Yes.
Event severity when service auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the a monitored service fails to restart. The default is 5.
Raise event if service auto-start succeeds?	Select **Yes** to raise an event when a monitored service successfully restarts. The default is Yes.
Event severity when service auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a monitored service successfully restarts. The default is 25.
Raise event if service auto-start is set to "n"?	Select **Yes** to raise an event when the *Auto-start the monitored services?* parameter is disabled. The default is Yes.
Event severity when service auto-start set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which the a *Auto-start the monitored services?* parameter is disabled. The default is 5.
Raise event if service doesn't exist?	Select **Yes** to raise an event when a monitored service does not exist. The default is Yes.
Event severity when service doesn't exist	Set the severity level, from 1 to 40, to indicate the importance of an event in which a monitored service does not exist. The default is 15.
Data Collection	
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns information about service status. The default is unselected.
Monitoring	
Auto-start the monitored services?	Select **Yes** to automatically start any monitored service that is down. The default is Yes.

Parameter	How To Set It
Monitor Cisco CRA Engine? (V3.x)	Select **Yes** to monitor the Cisco CRA Engine for Cisco UCCX version 3.x. The default is Yes.
Monitor Cisco CRS Node Manager? (V4.x)	Select **Yes** to monitor the Cisco CRS Node Manager for Cisco UCCX version 4.x. The default is Yes.
Additional V3.x Services	
Monitor Cisco AVVID Alarm?	Select **Yes** to monitor the Cisco AVVID Alarm. The default is unselected.
Monitor Cisco Purging Scheduler?	Select **Yes** to monitor the Cisco Purging Scheduler. The default is unselected.
Monitor Cisco CRA Servlet Engine?	Select **Yes** to monitor the Cisco CRA Servlet Engine. The default is unselected.
Monitor Cisco Desktop Enterprise Service?	Select **Yes** to monitor the Cisco Desktop Enterprise Service. The default is unselected.
Monitor Cisco Desktop RASCAL Service?	Select **Yes** to monitor the Cisco Desktop RASCAL Service. The default is unselected.
Monitor Cisco Desktop Sync Service?	Select **Yes** to monitor the Cisco Desktop Sync Service. The default is unselected.
Monitor Cisco Desktop TAI Service?	Select **Yes** to monitor the Cisco Desktop TAI Service. The default is unselected.
Monitor Cisco Desktop VoIP Monitor Service?	Select **Yes** to monitor the Cisco Desktop VoIP Monitor Service. The default is unselected.
Additional V4.x Services	
Monitor Cisco AVVID Alarm?	Select **Yes** to monitor the Cisco AVVID Alarm. The default is unselected.
Monitor Cisco Desktop Enterprise Service?	Select **Yes** to monitor the Cisco Desktop Enterprise Service. The default is unselected.
Monitor Cisco Desktop IP Phone Agent Service?	Select **Yes** to monitor the Cisco Desktop IP Phone Agent Service. The default is unselected.
Monitor Cisco Desktop LDAP Monitor Service?	Select **Yes** to monitor the Cisco Desktop LDAP Monitor Service. The default is unselected.
Monitor Cisco Desktop License and Resource Manager Service?	Select **Yes** to monitor the Cisco Desktop License and Resource Manager Service. The default is unselected.
Monitor Cisco Desktop Recording and Statistics Service?	Select **Yes** to monitor the Cisco Desktop Recording and Statistics Service. The default is unselected.
Monitor Cisco Desktop Recording Service?	Select **Yes** to monitor the Cisco Desktop Recording Service. The default is unselected.
Monitor Cisco Desktop Sync Service?	Select **Yes** to monitor the Cisco Desktop Sync Service. The default is unselected.
Monitor Cisco Desktop VoIP Monitor Service?	Select **Yes** to monitor the Cisco Desktop VoIP Monitor Service. The default is unselected.

ICD_MemoryHigh

Use this Knowledge Script to monitor the memory an application's processes are consuming. This script checks the memory used by each UCCX process individually, and the total memory used by all processes. If a process is not found, the script assumes the process is not running, and reports zero as the memory result.

Resource Object

Service child object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if service memory pool usage exceeds the threshold?	Select **Yes** to raise an event if the memory pool usage of a monitored service exceeds the threshold you set. The default is Yes.
Event severity when service memory pool usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the memory pool usage of a monitored service exceeds the threshold you set. The default is 10.
Raise event if service total memory usage exceeds the threshold?	Select **Yes** to raise an event if the total memory usage of a monitored service exceeds the threshold you set. The default is Yes.
Event severity when service total memory usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the total memory usage of a monitored service exceeds the threshold you set. The default is 10.
Data Collection	
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns memory usage data and memory pool usage data for the monitoring interval. The default is unselected.
Monitoring	
Version 3.x Services	
Monitor Cisco CRA Engine?	Select **Yes** to monitor the memory usage of Cisco CRA Engine. The default is Yes.
Threshold: Maximum Cisco CRA Engine memory usage	Specify the maximum amount of memory the Cisco CRA Engine can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco CRA Engine memory pool usage	Specify the maximum amount of memory pool the Cisco CRA Engine can consume before an event is raised. The default is 5000 KB.
Monitor Cisco AVVID Alarm?	Select **Yes** to monitor the memory usage of Cisco AVVID Alarm. The default is Yes.

Parameter	How To Set It
Threshold: Maximum Cisco AVVID Alarm memory usage	Specify the maximum amount of memory the Cisco AVVID Alarm can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco AVVID Alarm memory pool usage	Specify the maximum amount of memory pool the Cisco AVVID Alarm can consume before an event is raised. The default is 5000 KB.
Monitor Cisco Purging Scheduler?	Select **Yes** to monitor the memory usage of Cisco Purging Scheduler. The default is Yes.
Threshold: Maximum Cisco Purging Scheduler memory usage	Specify the maximum amount of memory the Cisco Purging Scheduler can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco Purging Scheduler memory pool usage	Specify the maximum amount of memory pool the Cisco Purging Scheduler can consume before an event is raised. The default is 5000 KB.
Monitor Cisco CRA Servlet Engine?	Select **Yes** to monitor the memory usage of Cisco CRA Servlet Engine. The default is Yes.
Threshold: Maximum Cisco CRA Servlet Engine memory usage	Specify the maximum amount of memory the Cisco CRA Servlet Engine can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco CRA Servlet Engine memory pool usage	Specify the maximum amount of memory pool the Cisco CRA Servlet Engine can consume before an event is raised. The default is 5000 KB.
Monitor Cisco Desktop Enterprise Service?	Select **Yes** to monitor the memory usage of Cisco Desktop Enterprise Service. The default is Yes.
Threshold: Maximum Cisco Desktop Enterprise Service memory usage	Specify the maximum amount of memory the Cisco Desktop Enterprise Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco Desktop Enterprise Service memory pool usage	Specify the maximum amount of memory pool the Cisco Desktop Enterprise Service can consume before an event is raised. The default is 5000 KB.
Monitor Cisco Desktop RASCAL Service?	Select **Yes** to monitor the memory usage of Cisco Desktop RASCAL Service. The default is Yes.
Threshold: Maximum Cisco Desktop RASCAL Service memory usage	Specify the maximum amount of memory the Cisco Desktop RASCAL Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco Desktop RASCAL Service memory pool usage	Specify the maximum amount of memory pool the Cisco Desktop RASCAL Service can consume before an event is raised. The default is 5000 KB.
Monitor Cisco Desktop Sync Service?	Select **Yes** to monitor the memory usage of Cisco Desktop Sync Service. The default is Yes.
Threshold: Maximum Cisco Desktop Sync Service memory usage	Specify the maximum amount of memory the Cisco Desktop Sync Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco Desktop Sync Service memory pool usage	Specify the maximum amount of memory pool the Cisco Desktop Sync Service can consume before an event is raised. The default is 5000 KB.
Monitor Cisco Desktop TAI Service?	Select **Yes** to monitor the memory usage of Cisco Desktop TAI Service. The default is Yes.

Parameter	How To Set It
Threshold: Maximum Cisco Desktop TAI Service memory usage	Specify the maximum amount of memory the Cisco Desktop TAI Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco Desktop TAI Service memory pool usage	Specify the maximum amount of memory pool the Cisco Desktop TAI Service can consume before an event is raised. The default is 5000 KB.
Monitor Cisco VoIP Monitor Service?	Select **Yes** to monitor the memory usage of Cisco VoIP Monitor Service. The default is Yes.
Threshold: Maximum Cisco VoIP Monitor Service memory usage	Specify the maximum amount of memory the Cisco VoIP Monitor Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco VoIP Monitor Service memory pool usage	Specify the maximum amount of memory pool the Cisco VoIP Monitor Service can consume before an event is raised. The default is 5000 KB.
Version 4.x Services	
Monitor Cisco CRS Node Manager?	Select **Yes** to monitor the memory usage of Cisco CRS Node Manager. The default is Yes.
Threshold: Maximum Cisco CRS Node Manager memory usage	Specify the maximum amount of memory the Cisco CRS Node Manager can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco CRS Node Manager memory pool usage	Specify the maximum amount of memory pool the Cisco CRS Node Manager can consume before an event is raised. The default is 5000 KB.
Monitor Cisco AVVID Alarm?	Select **Yes** to monitor the memory usage of Cisco AVVID Alarm. The default is Yes.
Threshold: Maximum Cisco AVVID Alarm memory usage	Specify the maximum amount of memory the Cisco AVVID Alarm can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco AVVID Alarm memory pool usage	Specify the maximum amount of memory pool the Cisco AVVID Alarm can consume before an event is raised. The default is 5000 KB.
Monitor Cisco Desktop Enterprise Service?	Select **Yes** to monitor the memory usage of Cisco Desktop Enterprise Service. The default is Yes.
Threshold: Maximum Cisco Desktop Enterprise Service memory usage	Specify the maximum amount of memory the Cisco Desktop Enterprise Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco Desktop Enterprise Service memory pool usage	Specify the maximum amount of memory pool the Cisco Desktop Enterprise Service can consume before an event is raised. The default is 5000 KB.
Monitor Cisco Desktop IP Phone Agent Service?	Select **Yes** to monitor the memory usage of Cisco Desktop IP Phone Agent Service. The default is Yes.
Threshold: Maximum Cisco Desktop IP Phone Agent Service memory usage	Specify the maximum amount of memory the Cisco Desktop IP Phone Agent Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco Desktop Enterprise Service memory pool usage	Specify the maximum amount of memory pool the Cisco Desktop Enterprise Service can consume before an event is raised. The default is 5000 KB.
Monitor Cisco Desktop LDAP Monitor Service?	Select **Yes** to monitor the memory usage of Cisco Desktop LDAP Monitor Service. The default is Yes.

Parameter	How To Set It
Threshold: Maximum Cisco Desktop LDAP Monitor Service memory usage	Specify the maximum amount of memory the Cisco Desktop LDAP Monitor Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco Desktop LDAP Monitor Service memory pool usage	Specify the maximum amount of memory pool the Cisco Desktop LDAP Monitor Service can consume before an event is raised. The default is 5000 KB.
Monitor Cisco Desktop License and Resource Manager Service?	Select **Yes** to monitor the memory usage of Cisco Desktop License and Resource Manager Service. The default is Yes.
Threshold: Maximum Cisco Desktop License and Resource Manager Service memory usage	Specify the maximum amount of memory the Cisco Desktop License and Resource Manager Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco Desktop License and Resource Manager Service memory pool usage	Specify the maximum amount of memory pool the Cisco Desktop License and Resource Manager Service can consume before an event is raised. The default is 5000 KB.
Monitor Cisco Desktop Recording and Statistics Service?	Select **Yes** to monitor the memory usage of Cisco Desktop Recording and Statistics Service. The default is Yes.
Threshold: Maximum Cisco Desktop Recording and Statistics Service memory usage	Specify the maximum amount of memory the Cisco Desktop Recording and Statistics Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco Desktop Recording and Statistics Service memory pool usage	Specify the maximum amount of memory pool the Cisco Desktop Recording and Statistics Service can consume before an event is raised. The default is 5000 KB.
Monitor Cisco Desktop Recording Service?	Select **Yes** to monitor the memory usage of Cisco Desktop Recording Service. The default is Yes.
Threshold: Maximum Cisco Desktop Recording Service memory usage	Specify the maximum amount of memory the Cisco Desktop Recording Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco Desktop Recording Service memory pool usage	Specify the maximum amount of memory pool the Cisco Desktop Recording Service can consume before an event is raised. The default is 5000 KB.
Monitor Cisco Desktop Sync Service?	Select **Yes** to monitor the memory usage of Cisco Desktop Sync Service. The default is Yes.
Threshold: Maximum Cisco Desktop Sync Service memory usage	Specify the maximum amount of memory the Cisco Desktop Sync Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco Desktop Sync Service memory pool usage	Specify the maximum amount of memory pool the Cisco Desktop Sync Service can consume before an event is raised. The default is 5000 KB.
Monitor Cisco VoIP Monitor Service?	Select **Yes** to monitor the memory usage of Cisco VoIP Monitor Service. The default is Yes.

Parameter	How To Set It
Threshold: Maximum Cisco VoIP Monitor Service memory usage	Specify the maximum amount of memory the Cisco VoIP Monitor Service can consume before an event is raised. The default is 200000 KB.
Threshold: Maximum Cisco VoIP Monitor Service memory pool usage	Specify the maximum amount of memory pool the Cisco VoIP Monitor Service can consume before an event is raised. The default is 5000 KB.

ICD_RestartService

Use this Knowledge Script to schedule a UCCX service to stop and then start after a specified interval. This script raises an event if a service should not be restarted, if a service fails to restart, if a service has a status of "Started," if a service is missing, if a service stopped normally, or if no status information can be retrieved for a service. In addition, this script generates data streams for the number of successful service starts and stops.

Resource Object

Service child object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if service is down and should not be restarted?	Select **Yes** to raise an event when a monitored service is down and should not be restarted. The default is Yes.
Event severity when service is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service is down and should not be restarted. The default is 10.
Raise event if service fails to start?	Select **Yes** to raise an event when a monitored service fails to restart. The default is Yes.
Event severity when service fails to start	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service fails to restart. The default is 15.
Raise event if status of service is "Started"?	Select **Yes** to raise an event when a monitored service has a status of "Started." The default is Yes.
Event severity when status of service is "Started"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service has a status of "Started". The default is 25.
Raise event if service is missing?	Select **Yes** to raise an event when a monitored service is missing. The default is Yes.
Event severity when service is missing	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service is missing. The default is 15.
Raise event if service is disabled?	Select **Yes** to raise an event when a monitored service has been disabled. The default is Yes.
Event severity when service is disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service has been disabled. The default is 15.
Raise event if service is shut down normally?	Select **Yes** to raise an event when a monitored service has shut down normally. The default is Yes.
Event severity when service is shut down normally	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service has shut down normally. The default is 25.

Parameter	How To Set It
Raise event if unable to retrieve service status?	Select **Yes** to raise an event in which AppManager is unable to retrieve the status of a monitored service. The default is Yes.
Event severity when unable to retrieve service status	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager is unable to retrieve the status of a monitored service. The default is 5.
Data Collection	
Collect data?	Select **Yes** to collect data about any of the monitored services. The default is unselected.
Monitoring	
Version 3.x Services	
Restart Cisco CRA Engine?	Select **Yes** to restart Cisco CRA Engine. The default is Yes.
Restart Cisco AVVID Alarm?	Select **Yes** to restart Cisco AVVID Alarm. The default is Yes.
Restart Cisco Purging Scheduler?	Select **Yes** to restart Cisco Purging Scheduler. The default is Yes.
Restart Cisco CRA Servlet Engine?	Select **Yes** to restart Cisco CRA Servlet Engine. The default is Yes.
Restart Cisco Desktop Enterprise Service?	Select **Yes** to restart Cisco Desktop Enterprise Service. The default is Yes.
Restart Cisco Desktop RASCAL Service?	Select **Yes** to restart Cisco Desktop RASCAL Service. The default is Yes.
Restart Cisco Desktop Sync Service?	Select **Yes** to restart Cisco Desktop Sync Service. The default is Yes.
Restart Cisco Desktop TAI Service?	Select **Yes** to restart Cisco Desktop TAI Service. The default is Yes.
Restart Cisco Desktop VoIP Monitor Service?	Select **Yes** to restart Cisco Desktop VoIP Monitor Service. The default is Yes.
Version 4.x Services	
Restart Cisco CRS Node Manager?	Select **Yes** to restart Cisco CRS Node Manager. The default is Yes.
Restart Cisco AVVID Alarm?	Select **Yes** to restart Cisco AVVID Alarm. The default is Yes.
Restart Cisco Desktop Enterprise Service?	Select **Yes** to restart Cisco Desktop Enterprise Service. The default is Yes.
Restart Cisco Desktop IP Phone Agent Service?	Select **Yes** to restart Cisco Desktop IP Phone Agent Service. The default is Yes.
Restart Cisco Desktop LDAP Monitor Service?	Select **Yes** to restart Cisco Desktop LDAP Monitor Service. The default is Yes.
Restart Cisco Desktop License and Resource Manager Service?	Select **Yes** to restart Cisco Desktop License and Resource Manager Service. The default is Yes.
Restart Cisco Desktop Recording and Statistics Service?	Select **Yes** to restart Cisco Desktop Recording and Statistics Service. The default is Yes.
Restart Cisco Desktop Recording Service?	Select **Yes** to restart Cisco Desktop Recording Service. The default is Yes.

Parameter	How To Set It
Restart Cisco Desktop Sync Service?	Select **Yes** to restart Cisco Desktop Sync Service. The default is Yes.
Restart Cisco Desktop VoIP Monitor Service?	Select **Yes** to restart Cisco Desktop VoIP Monitor Service. The default is Yes.
Start down services?	Select **Yes** to start any monitored service that is down. The default is Yes.
Start dependent services? (6.0+)	Select **Yes** to start any dependent service that is down. The default is Yes. Applies only to versions 6.0 and above.
Service start timeout	Specify the maximum number of seconds that are allowed for a service to restart. If the specified time elapses and the service has not restarted, an event will be raised. The default is 30 seconds.
Restart service if shutdown is normal?	Select **Yes** to restart a service that has shut down normally. The default is Yes.
Wait N seconds before restarting service	Specify the number of seconds that should elapse before a service is restarted. The default is 10 seconds.

ICD_SystemUsage

Use this Knowledge Script to monitor the amount of CPU and memory that the Cisco CRA Engine process is using.

If the CPU usage (%) for the Cisco CRA Engine process or total CPU usage (%) exceeds a threshold, an event is raised. If memory pool usage (KB) for the Cisco CRA Engine process or total memory usage (KB) exceed their respective thresholds, an event is raised. Also, if data collection is enabled, data streams are generated for Cisco CRA Engine CPU usage, total CPU usage, Cisco CRA Engine memory pool usage, and total memory usage.

Resource Object

Cisco ICD parent object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if CPU usage exceeds the threshold?	Select **Yes** to raise an event when CPU usage exceeds the threshold you set. The default is Yes
Event severity when CPU utilization exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold you set. The default is 15.
Raise event if memory usage exceeds the threshold?	Select **Yes** to raise an event when memory usage exceeds the threshold you set. The default is Yes.
Event severity when memory usage exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for CPU usage?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of CPU usage for the monitoring period. The default is unselected.
Collect data for memory usage	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the amount of memory usage, in KB, for the monitoring period. The default is unselected.
Monitoring	
Threshold: Maximum Cisco ICD Engine CPU usage	Specify the highest amount of CPU that the Cisco UCCX Engine can consume before an event is raised. The default is 65%.
Threshold: Maximum total CPU usage	Specify the highest amount of CPU that the entire UCCX system can consume before an event is raised. The default is 80%.

Parameter	How To Set It
Threshold: Maximum Cisco ICD Engine memory pool usage	Specify the highest amount of memory pool that the Cisco UCCX Engine can consume before an event is raised. The default is 65%.
Threshold: Maximum Cisco ICD Engine total memory usage	Specify the highest amount of memory that the Cisco UCCX Engine can consume before an event is raised. The default is 80%.

IIS_CpuHigh

Use this Knowledge Script to monitor CPU usage for IIS application processes. This script raises an event if a threshold is exceeded. In addition, this script generates a data stream for CPU usage (%).

Resource Object

IIS server object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if CPU usage exceeds the threshold?	Select **y** to raise an event if CPU usage exceeds the threshold you set. The default is y.
Collect data?	Select **y** to collect data for charts and reports. When enabled, data collection returns the percentage of CPU usage for the monitoring period. The default is n.
Process names	Provide the names of the application processes you want to monitor. Separate multiple entries with commas. For example: `inetinfo,dllhost`. The default is inetinfo. **Note** Do not append .exe to the process names.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU resources the selected process can consume before an event is raised. The default is 60%.
Event severity when CPU usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 15.

IIS_HealthCheck

Use this Knowledge Script to check IIS servers, Web site status, and the queue length for blocked I/O requests. If any server or Web site is not running, an event is raised. In addition, you can choose to automatically restart the IIS server or Web site. This script raises an event if the blocked I/O queue length is longer than the specified threshold.

This script monitors only Web sites (servers), not FTP sites, NNTP sites, or SMTP sites.

Resource Object

IIS server object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Auto-start monitored server(s)?	Select **y** to automatically restart down servers. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which monitored server fails to start. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a monitored server starts successfully. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and the *Auto-start monitored servers?* parameter is set to n. The default is 18.
Event severity for blocked I/O requests	Set the event severity level, from 1 to 40, to indicate the importance of an event in which blocked I/O requests are in queue. The default is 5.
Threshold - Maximum blocked I/O requests	Specify the maximum number of blocked I/O requests that can be in the queue before an event is raised. The default is zero requests.
Monitor IIS server?	Select **y** to monitor the IIS server. The default is y.
Monitor FTP server?	Select **y** to monitor the FTP server. The default is n.

IIS_KillTopCPUProcs

Use this Knowledge Script to monitor the CPU usage for the IIS `dllhost` and `mtx` processes. This script raises an event if a threshold is exceeded. You can set this script to automatically stop a process that exceeds the CPU usage threshold.

Resource Object

IIS server object

Default Schedule

By default, this script runs every three minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if kill is successful or unsuccessful?	Select **y** to raise an event if the stop process is successful or unsuccessful. The default is y.
Kill CPU-intensive processes?	Select **y** to automatically stop any process that exceeds the CPU usage threshold. The default is n.
Threshold - Maximum CPU usage allowed	Specify the maximum percentage of CPU the `dllhost` and `mtx` processes can consume before an event is raised. The default is 90%.
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 10.
Event severity when kill fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a process exceeds the threshold and AppManager cannot stop the process. The default is 10.
Event severity when kill succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a process exceeds the threshold and AppManager has successfully stopped the process. The default is 20.

IIS_MemoryHigh

Use this Knowledge Script to monitor memory usage for selected IIS application processes. This script raises an event memory usage exceeds the threshold you set. In addition, this script generates a data stream for memory usage (%).

Resource Object

IIS server object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold exceeded?	Select **y** to raise an event when memory usage exceeds the threshold you set. The default is y.
Collect data?	Select **y** to collect data for charts and reports. When enabled, data collection returns the named process's memory usage during the monitoring interval. The default is n.
Process names	Provide the name of the application process you want to monitor. Use a comma to separate multiple entries — do not use spaces. For example: `inetinfo,dllhost`. The default is `inetinfo`. **Note** Do not append .exe to the process names.
Threshold - Maximum memory usage	Specify the maximum amount of memory the selected process can consume before an event is raised. The default is 10000000 bytes.
Threshold - Maximum memory pool usage	Specify the maximum amount of memory pool the selected process can consume before an event is raised. The default is 5000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. The default is 15.

IIS_ServiceUpTime

Use this Knowledge Script to monitor the uptime for Web sites and services. This script raises an event if the amount of time the sites and services are running is less than the threshold you set. In addition, this script generates a data stream the length of time a service has been running.

Prerequisite

The server on which you run this script must be running IIS version 5 or later.

Resource Objects

IIS Web server or FTP server object

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if uptime falls below threshold?	Select **y** to raise an event if uptime falls below the threshold. The default is y.
Collect data?	Select **y** to collect data for charts and reports. When enabled, data collection returns the number of seconds a service has been running during the monitoring interval. The default is n.
Threshold - Minimum uptime	Specify the minimum amount of time that discovered Web site/services and FTP sites/services are required to be running to prevent an event from being raised. The default is 10000 seconds.
Event severity when uptime falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which uptime falls below the threshold. The default is 5.

SQL_Accessibility

Use this Knowledge Script to monitor SQL Server and database accessibility. This script raises an event if a SQL Server or a specified database is not accessible. In addition, this script can generate data streams for database accessibility.

Resource Object

Cisco ICD SQL Server object

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if SQL Server or specified database not accessible	Select **Yes** to raise an event if SQL Server or the specified database is not accessible. The default is *s.*
Event severity when SQL Server or specified database not accessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which SQL Server or the database is not accessible. The default is 5.
Data Collection	
Collect data?	Select **Yes** to collect data for reports and graphs. If y selected, this script returns 100 if all specified databases are accessible, 50 if some of the specified databases are accessible and some are not, or 0 if none of the specified databases is accessible. The default is unselected.
Monitoring	
Response timeout before target inaccessible	Enter a timeout period in seconds. The timeout period is the number of seconds to wait for a response before retrying or determining the target database is inaccessible. The default is zero seconds. **Note** When specifying a timeout, the Knowledge Script continues waiting until it receives a response or the timeout is reached. During this waiting period, other jobs are blocked from execution. Therefore, limit use of this parameter or keep the timeout period at a minimum for regular monitoring jobs. (When you are running this script to troubleshoot a particular problem and not as part of a regularly scheduled interval for ongoing maintenance, you can adjust this parameter to allow a longer time out period.)
Number of retries before target inaccessible	Enter the number of times to retry connecting to the target database before determining the database is inaccessible. The default is zero retries. **Note** When specifying this parameter the script continues waiting until it receives a response or has made the specified number of retry attempts. During this waiting period, other jobs are blocked from execution. Therefore, limit use of this parameter or keep retry attempts at a minimum for regular monitoring jobs. (When you are running this script to troubleshoot a particular problem and not as part of a regularly scheduled interval for ongoing maintenance, you can adjust this parameter to allow more retry attempts.)

Parameter	How To Set It
SQL username	Enter the database name that you want to use to access SQL Server. The username you enter must have permission to access the database names for which you want to check accessibility. To use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Database name	Enter the database names for which you want to check access, separated by commas. For example, enter `master,pubs,tempdb`. If you leave this field blank, the script checks access to all databases. The default is master.

SQL_CPUUtil

Use this Knowledge Script to monitor the percentage of CPU resources used by the `sqlservr` and `sqlagent` processes. This script raises an event if the CPU usage exceeds the threshold you set. In addition, this script generates data streams for CPU usage (%).

Resource Object

Cisco ICD SQL Server object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if the SQL Server process exceeds the threshold?	Select **Yes** to raise an event if SQL Server CPU usage exceeds the threshold. The default is y.
Event severity when the SQL Server process exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which SQL Server CPU usage exceeds the threshold. The default is 8.
Raise event if the SQL Agent process exceeds the threshold?	Select **Yes** to raise an event if SQL Agent CPU usage exceeds the threshold. The default is y.
Event severity when SQL Agent process exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which SQL Agent CPU usage exceeds the threshold. The default is 8.
Data Collection	
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns process CPU usage for the monitoring period. The default is unselected.
Monitoring	
Threshold - Maximum CPU usage for SQL Server process	Specify the maximum amount of CPU that the SQL Server process can consume before an event is raised. The default is 10%.
Threshold - Maximum CPU usage for SQL Agent process	Specify the maximum amount of CPU that the SQL Agent process can consume before an event is raised. The default is 10%.

SQL_DataGrowthRate

Use this Knowledge Script to monitor the data growth and shrink rates for all SQL Server databases. Growth and shrink rates are calculated by taking the difference between the data space utilization from the current interval and the data space utilization from the last interval. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for growth and shrink rates.

Resource Object

Cisco ICD SQL Server database object

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if data growth rate exceeds the threshold	Select **Yes** to raise an event if the data growth rate exceeds the threshold. The default is Yes.
Event severity when data growth rate exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data growth rate exceeds the threshold. The default is 5.
Raise event if data shrink rate exceeds the threshold	Select **Yes** to raise an event if the data shrink rate exceeds the threshold. The default is Yes.
Event severity when data shrink rate exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data shrink rate exceeds the threshold. The default is 5.
Data Collection	
Collect data?	Select **Yes** to collect data about growth and shrink rates for reports and graphs. The default is unselected.
Monitoring	
Dynamically enumerate at each interval	Select **Yes** to dynamically enumerate databases at each monitoring interval. The default is y. To dynamically enumerate a database means that each time it runs, AppManager automatically determines and reports on all existing databases. Information is returned even for databases that are not yet discovered.
Exclude these objects	Provide the names of objects you want to exclude from dynamic enumeration. You can exclude multiple objects, separated by commas with no spaces. For example, enter `master,model,mdb` **Note** Ignore this parameter if you are not dynamically enumerating databases.
Threshold - Maximum data growth rate	Specify the maximum percentage of data growth that is allowed between the last and current interval before an event is raised. Enter 0 to ignore this parameter. The default is 25%.

Parameter	How To Set It
Threshold - Maximum data shrink rate	Specify the maximum percentage of data shrinkage that is allowed between the last and current intervals before an event is raised. Enter 0 to ignore this parameter. The default is 25%.
SQL username	Specify the database username account that you want to use to access SQL Server. You can use the "sa" account or other user login accounts that have been set up in the managed client's SQL Server. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use. **Note** If you are monitoring SQL Server 7, to use a `sysadmin` role account. Only members of the *sysadmin* role can retrieve file statistics on SQL Server 7.0.

SQL_DBGrowthRate

Use this Knowledge Script to monitor database growth and shrink rates. Growth and shrink rates are calculated by taking the difference between the database space utilization from the current interval and the database space utilization from the last interval. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for growth and shrink rates.

Resource Object

Cisco ICD SQL Server database object

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if database growth rate exceeds the threshold?	Select **Yes** to raise an event if the database growth rate exceeds the threshold. The default is Yes.
Event severity when database growth rate exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the database growth rate exceeds the threshold. The default is 5.
Raise event if database shrink rate exceeds the threshold?	Select **Yes** to raise an event if the database shrink rate exceeds the threshold. The default is Yes.
Event severity when database shrink rate exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the database shrink rate exceeds the threshold. The default is 5.
Data Collection	
Collect data?	Select **Yes** to collect data about growth and shrink rates for reports and graphs. The default is Yes.
Monitoring	
Dynamically enumerate at each interval	Select **Yes** to dynamically enumerate databases at each monitoring interval. The default is y. To dynamically enumerate a database means that each time it runs, AppManager automatically determines and reports on all existing databases. Information will be returned even for databases that are not yet discovered in the TreeView pane.
Exclude these objects	Provide the names of objects you want to exclude from dynamic enumeration. You can exclude multiple objects, separated by commas with no spaces. For example, enter `master,model,mdb` **Note** Ignore this parameter if you are not dynamically enumerating databases.
Threshold - Maximum database growth rate	Specify the maximum percentage of database growth that is allowed between the last and current intervals before an event is raised. Enter 0 to ignore this parameter. The default is 25%.

Parameter	How To Set It
Threshold - Maximum database shrink rate	Specify the maximum percentage of database shrinkage that is allowed between the last and current intervals before an event is raised. Enter 0 to ignore this parameter. The default is 25%.
SQL username	Specify the database username that you want to use to access SQL Server. You can use the "sa" account or other user login accounts that have been set up in the managed client's SQL Server. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use. **Note** If you are monitoring SQL Server 7, use a `sysadmin` role account. Only members of the `sysadmin` role can retrieve file statistics on SQL Server 7.0.
Update usage?	Select **Yes** to have SQL Server recalculate the space usage. The default is unselected.

SQL_MemUtil

Use this Knowledge Script to monitor the amount of memory that is used by the processes: `sqlservr` and `sqlagent` processes

If using SQL Server 7.0 or 2000, you can use this script to monitor total server memory usage, number of free buffers, and memory usage.

This script raises an event if the amount of memory used by SQL Server exceeds the threshold you set. In addition, this script can generate data streams for memory usage (%).

Resource Object

Cisco ICD SQL Server object

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if SQL process memory usage exceeds the threshold?	Select **Yes** to raise an event if sqlagent memory usage exceeds the threshold you set. The default is Yes.
Event severity when SQL process memory usage exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which sqlagent memory usage exceeds the threshold. The default is 5.
Raise event if free buffer count falls below the threshold?	Select **Yes** to raise an event if the number of free buffers falls below the threshold you set. The default is Yes.
Event severity when free buffer count falls below the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of free buffers falls below the threshold. The default is 5.
Raise event if SQL Server memory usage exceeds the threshold?	Select **Yes** to raise an event if the sqlservr memory usage exceeds the threshold. The default is Yes.
Event severity when SQL Server memory usage exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which sqlservr memory usage exceeds the threshold. The default is 5.
Data Collection	
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns sqlservr and sqlagent memory usage for the monitoring period. The default is n.
Threshold - Maximum process memory usage	Specify the maximum amount of memory that can be consumed by the SQL process before an event is raised. The default is 50000000 bytes.

Parameter	How To Set It
Threshold - Minimum free buffers available	Specify the minimum number of buffers that must be available to prevent an event from being raised. The default is 50 buffers.
Threshold - Maximum SQL Server memory usage	Specify the maximum amount of memory that can be in use by SQL Server and all related processes before an event is raised. The default is 30000000 bytes.

SQL_RestartServer

Use this Knowledge Script to restart a SQL server and stop dependent UCCX services. These services will automatically be restarted. This script raises an event if the server either successfully restarts or fails to restart.

Resource Object

Cisco ICD SQL Server object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event Notification	
Raise event if stop fails?	Select **Yes** to raise an event if AppManager cannot stop the service. The default is Yes.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the service. The default is 5.
Raise event if start fails?	Select **Yes** to raise an event if AppManager cannot start the service. The default is Yes.
Event severity when start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot start the service. The default is 5.
Raise event if status of service is unavailable?	Select **Yes** to raise an event if AppManager cannot determine the status of the service. The default is Yes.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the service. The default is 10.
Raise event if stop succeeds?	Select **Yes** to raise an event if AppManager successfully stops the service. The default is Yes.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the service. The default is 25.
Raise event if restart succeeds?	Select **Yes** to raise an event if AppManager successfully restarts the service. The default is Yes.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the service. The default is 25.
Monitoring	
Wait N seconds before restarting service	Specify the number of seconds to wait after the server is stopped before attempting to restart the service. The default is 5 seconds.

Recommended Knowledge Script Group

The following Knowledge Scripts are members of the CiscoICD recommended Knowledge Script Group (KSG).

- CallStatistics
- CSQ_ServiceLevel
- ICD_HealthCheck
- ICD_SystemUsage
- SQL_DBGrowthRate

The parameters of all scripts in the KSG are set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and run the CiscoICD group on a Unified Contact Center Express (UCCX) resource.

Run the KSG on only one cluster at a time. Running the KSG on multiple clusters all at once hinders the proxy agent's ability to spread out processing over time. You can monitor multiple clusters by running the KSG on the first cluster, and then repeating the process for each additional cluster.

The CiscoICD KSG provides a "best practices" usage of AppManager for monitoring your UCCX environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView. For more information, see "About Policy-Based Monitoring" in the AppManager Help.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the CiscoICD tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoICD tab are not affected.

When deployed as part of a KSG, a script's default script parameter settings may differ from when the script is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the CiscoICD KSG and want to restore it to its original form, you can reinstall the AppManager for Cisco Integrated Contact Distribution module on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\CiscoICD\RECOMMENDED_CiscoICD` directory.

Chapter 22
CiscoICM Knowledge Scripts

Cisco Intelligent Contact Management is now known as Cisco Unified Contact Center Enterprise (UCCE). UCCE provides contact routing and call treatment across several geographically distributed call centers over an IP infrastructure.

AppManager Knowledge Scripts retrieve information from UCCE computers to help you better manage UCCE. You can use the retrieved information to identify when services are down, when events have been logged, and when performance-monitoring data exceeds thresholds.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ICM_AgentData	Monitors agent data from the UCCE database.
ICM_Alarms	Monitors the UCCE server for error, warning, and informational alarms.
ICM_EventGetViaFilter	Returns a formatted text version of matching events from the UCCE database, not the Windows event log.
ICM_EventLog	Monitors event log entries from UCCE during the past *n* hours.
ICM_ProcessLog	Searches a log file for a particular regular expression.
ICM_RouteData	Monitors Route data from the UCCE database.
ICM_RoutingClientData	Monitors Routing Client data from the UCCE database.
ICM_ScheduledTargetDataLocal	Monitors Scheduled Target data from the UCCE local database.
ICM_ScriptData	Monitors Script data from the UCCE database.
ICM_ServiceData	Monitors Service data from the UCCE database.
ICM_ServiceDataLocal	Monitors Service data from the UCCE local database.
ICM_SkillGroupData	Monitors Skill Group data from the UCCE database.
ICM_SkillGroupDataLocal	Monitors Skill Group data from the UCCE local database.
IIS_CpuHigh	Monitors CPU usage for IIS processes.
IIS_HealthCheck	Monitors the queue length for blocked I/O requests and the up-and-down status of IIS services and Web sites.
IIS_KillTopCPUProcs	Monitors the CPU usage of the dllhost and MTX processes.
IIS_MemoryHigh	Monitors memory usage and memory pool usage for IIS application processes.
IIS_RestartServer	Restarts an IIS server.
IIS_ServiceUpTime	Monitors uptime for Web sites and Web services.

Knowledge Script	What It Does
Router_AgentsLoggedOn	Monitors the total number of agents currently logged on to a router.
Router_CallsInProgress	Monitors the total number of calls in progress for a router.
Router_CallsPerSec	Monitors the number of calls per second for a router. I
SQL_Accessibility	Monitors whether the SQL Server database is accessible.
SQL_CPUUtil	Monitors CPU usage by SQL Server processes.
SQL_DataGrowthRate	Monitors data growth and shrink rates for all SQL Server databases.
SQL_DBGrowthRate	Monitors database growth and shrink rates.
SQL_MemUtil	Monitors memory usage by SQL Server processes.
SQL_RestartServer	Restarts a SQL Server computer.
Recommended Knowledge Script Group	Performs essential monitoring of your UCCE environment.

ICM_AgentData

Use this Knowledge Script to monitor agent data from the UCCE database. A separate event or data stream is generated for each agent. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for each monitored metric.

Resource Object

CISCOICM_CentralDB

Default Schedule

By default, this script runs every 30 minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you specify 15, the script will search through the most recent 15 minutes of activity. The default is 60 minutes. **Note** Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.

Parameter	How To Set It
On subsequent runs, query database for extended time range?	Select **Yes** to search the database beginning with records that have timestamps that fall within a time range based on twice the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:15 through 9:45. In other words, the query searches 30 minutes' worth of records beginning 60 minutes (twice the Schedule) prior to the time the job runs. Disable this option to search the database beginning with records that have timestamps that fall within a time range that is the same as the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:45 through 10:15. In other words, the query searches the most recent 30 minutes' worth of records. **Important** Select the option appropriate for your UCCE environment. In newer versions of UCCE, records are not inserted in the database until 30 minutes after the timestamp. Therefore, a record with a timestamp of 9:00 is not inserted into the database until 9:30. This Knowledge Script queries for records that have timestamps that fall within the time frame of the query. To capture records that undergo a 30-minute delay between timestamp and database insertion, select **Yes**.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. To use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum agent logged-on time	Specify the maximum amount of time that agents can be logged on before an event is raised. The default is 1680 seconds.
Event severity when logged-on time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which logged-on time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for agent logged-on time?	Set to **y** to collect data about the amount of time that agents are logged on. The default is n.
Threshold - Maximum agent available time	Specify the maximum amount of time that agents can be available before an event is raised. The default is 1680 seconds.
Event severity when available time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which available time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for agent available time?	Set to **y** to collect data about the amount of time that agents are available. The default is n.
Threshold - Maximum agent not-ready time	Specify the maximum amount of time that agents can be in a Not Ready state before an event is raised. The default is 120 seconds.
Event severity when not-ready time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which not-ready time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for agent not-ready time	Set to **y** to collect data about the amount of time that agents are in a Not Ready state. The default is n.

ICM_Alarms

Use this Knowledge Script to monitor the log on the Cisco UCCE server for error, warning, and informational alarms. You can filter alarms by severity and alarm identifier. This script raises an event if an alarm is detected. An event's short message contains the alarm identifier in the following format: `component_id:alarm_id`. For example, `4_5_IPCC-RGRA_ICM\netiq\LoggerA:0xA1028105`.

Resource Object

CISCOICM

Default Schedule

By default, this script runs on an asynchronous schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ICM_Alarms job fails for an unexpected reason. The default is 5.
Monitor Error Alarms?	Set to **Yes** to monitor the UCCE log for error alarms. The default is Yes.
Include or exclude alarms	Select **Include only** to monitor *only* the error alarm identifiers you specify in the *Alarm identifiers* parameter. Select **Exclude** to exclude the specified error alarm identifiers from monitoring. The default is Exclude.
Alarm identifiers	Type a comma-separated list of the error alarm identifiers you want to include in or exclude from monitoring. The default is an empty list.
Event Notification	
Raise event if error alarms are detected?	Set to **Yes** to raise an event if the UCCE log contains error alarms. The default is Yes.
Event severity when error alarms are detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which an error alarm is found in the UCCE log. The default is 10.
Monitor Warning Alarms?	Set to **Yes** to monitor the UCCE log for warning alarms. The default is unchecked.
Include or exclude alarms	Select **Include only** to monitor *only* the warning alarm identifiers specified in the following parameter. Select **Exclude** to exclude the specified warning alarm identifiers from monitoring. The default is Exclude.
Alarm identifiers	Type a comma-separated list of the warning alarm identifiers you want to include in or exclude from monitoring. The default is an empty list.
Event Notification	

Parameter	How To Set It
Raise event if warning alarms are detected?	Set to **Yes** to raise an event if the UCCE log contains warning alarms. The default is Yes.
Event severity when warning alarms are detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which a warning alarm is found in the UCCE log. The default is 15.
Monitor Informational Alarms?	Set to **Yes** to monitor the UCCE log for informational alarms. The default is unchecked.
Include or exclude alarms	Select **Include only** to monitor *only* the informational alarm identifiers specified in the following parameter. Select **Exclude** to exclude the specified informational alarm identifiers from monitoring. The default is Exclude.
Alarm identifiers	Type a comma-separated list of the informational alarm identifiers you want to include in or exclude from monitoring. The default is an empty list.
Event Notification	
Raise event if informational alarms are detected?	Set to **Yes** to raise an event if the UCCE log contains informational alarms. The default is Yes.
Event severity when informational alarms are detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which an informational alarm is found in the UCCE log. The default is 20.

ICM_EventGetViaFilter

Use this Knowledge Script to create a formatted text version of matching events. These events are from the UCCE database, not the Windows event log. This script raises separate events for each event found in the database.

Resource Object

CISCOICM_CentralDB

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Set this parameter to determine which events are searched the first time you run the Knowledge Script job. The default is 30 minutes. Subsequent searches begin where the previous one finished. The following entries are valid: • **n** to search entries for the past n minutes (8 for the past 8 minutes, 50 for the past 50 minutes, etc.) • **0** to search no previous entries (search from the current time forward) **Note** Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
Cisco ICM database username	Enter the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Event severity for error message	Set the severity level, from 1 to 40, to indicate the importance of an event in which an error message is found in the UCCE database. The default is 10.
Event severity for warning message	Set the severity level, from 1 to 40, to indicate the importance of an event in which a warning message is found in the UCCE database. The default is 20.
Event severity for informational message	Set the severity level, from 1 to 40, to indicate the importance of an event in which an informational message is found in the UCCE database. The default is 30.

ICM_EventLog

Use this Knowledge Script to monitor event log entries from the UCCE database during the past *n* hours. This script raises an event if log entries are detected. In addition, this script generates data streams for log entries.

Resource Object

CISCOICM

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event for log entries?	Set to **y** to raise an event when the log contains entries for which you have filtered. The default is y.
Collect data?	Set to **y** to collect data about log entries for charts and graphs. The default is n.
Separate data?	Set to **y** to separate events entries from different log files into different data streams. If set to **n**, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. The default is n. For example, if you are monitoring both the System and Application logs, you may want to set this parameter to **y** so that events in the System log are tracked separately from events in the Application log.
Log source	Specify the event log you want to monitor. You can specify multiple event logs, separated by commas. For example: `System,Application`. The default is Application.
Type: Error	Set to **y** to monitor for error events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is y.
Type: Warning	Set to **y** to monitor for warning events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is y.
Type: Information	Set to **y** to monitor for information events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is n.
Type: Success Audit	Set to **y** to monitor for success audit events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is n.
Type: Failure Audit	Set to **y** to monitor for failure audit events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is n.

Parameter	How To Set It
Instructions for filters: To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log. The search string can contain criteria used to include entries, exclude entries, or both.· • Separate include and exclude criteria with a colon (:). For example, `net:logon`. • Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ`. • If you specify only include criteria, the colon is not necessary. For example, `SQL`. • If you specify only exclude criteria, start the search string with a colon. For example, `:defragmentation,cleanup`.	
Event source filter	Specify one or more text strings to look for; separate multiple strings with commas. If your valid text string includes a comma, replace the comma with a tilde. For example: `GeoTel ICR,Cisco Systems~Inc.` The Knowledge Script will convert the tilde to a comma at runtime.
Event category filter	Specify one or more text strings to look for; separate multiple strings with commas.
Event ID filter	Specify a single event ID or a range of event IDs; separate multiple entries by commas. For example: `1094,1404-1463`
Event user filter	Specify a single or multiple user names to look for; separate multiple entries by commas. For example: `Pat,Chris,Alex`
Computer filter	Specify a single or multiple computer names to look for; separate multiple entries by commas. For example: `SHASTA,MARS`
Event description filter	Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods; separate multiple entries with commas. For example: `data loss during system failures,corrupt indices,Inter-Site Transport objects failed`
Maximum number of entries per event report	Specify the maximum number of Application log events that can be returned in each event report. For example, if this value is set to 30 and 67 Application log events are found, three event reports are raised: two reports containing 30 events and one report containing seven events. The default is 30. The Message column on the Events tab in the Operator Console displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.
Event severity for log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event. You may want to adjust the severity depending on the types of events for which you are checking. The default is 15.

ICM_ProcessLog

The UCCE Event Management System (EMS) logs events from processes throughout the system and stores the event data in the central database.

The EMS also saves events from individual processes in per-process log files on the local computer. These files document events for a specific process running on a specific computer. Use this Knowledge Script to search a log file for a particular regular expression.

Prerequisite

The UCCE computer on which you run this script must be running Internet Explorer 5.5 or later.

Resource Object

CiscoICM_Process

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event for log entries?	Set to **y** to raise an event if the log contains entries for which you have filtered. The default is y.
Collect data for log entries?	Set to **y** to collect data about log entries for reports and graphs. The default is n.
On first run, minutes to go back	Set this parameter to determine which events are searched the first time you run the Knowledge Script job. The default is 30 minutes. Subsequent searches begin where the previous one finished. The following entries are valid: • **n** to search entries for the past n minutes (8 for the past 8 minutes, 50 for the past 50 minutes, etc.) • **0** to search no previous entries (search from the current time forward) **Note** Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
Filter (regular expression)	Enter the expression by which you want to filter the process log. The default is error|warning|failed|unexpected.
Event severity when log entries present	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the log contains entries for which you have filtered. The default is 10.
Preceding lines to include	Enter the number of lines to include before the matching entry in the event text. The default is 2.

Parameter	How To Set It
Following lines to include	Enter the number of lines to include after the matching entry in the event text. The default is 2.

ICM_RouteData

Use this Knowledge Script to monitor data from the Route_Half_Hour table in the UCCE database. This script raises an event if a threshold is exceeded. In addition, this script generates separate data streams for each agent.

Resource Object

CISCOICM_CentralDB

Default Schedule

By default, this script runs every 30 minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database.For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 60. **Note** Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
On subsequent runs, query database for extended time range?	Select **Yes** to search the database beginning with records that have timestamps that fall within a time range based on twice the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:15 through 9:45. In other words, the query searches 30 minutes' worth of records beginning 60 minutes (twice the Schedule) prior to the time the job runs. Disable this option to search the database beginning with records that have timestamps that fall within a time range that is the same as the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:45 through 10:15. In other words, the query searches the most recent 30 minutes' worth of records. **Important** Select the option appropriate for your UCCE environment. In newer versions of UCCE, records are not inserted in the database until 30 minutes after the timestamp. Therefore, a record with a timestamp of 9:00 is not inserted into the database until 9:30. This Knowledge Script queries for records that have timestamps that fall within the time frame of the query. To capture records that undergo a 30-minute delay between timestamp and database insertion, select **Yes**.

Parameter	How To Set It
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum handled calls	Specify the maximum amount of calls that can be handled before an event is raised. The default is 200 calls.
Event severity when handled calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of handles calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for handled calls?	Set to **y** to collect data about handled calls for reports and graphs. The default is n.
Threshold - Service Level	Specify your UCCE Service Level threshold, which is the percentage of calls that are answered within the number of seconds you set as a goal for connecting a call with an agent. If the Service Level threshold is exceeded, an event is raised. The default is 20%.
Event severity when Service Level threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Service Level threshold is exceeded. Set to **0** if you want to ignore the event. The default is 20.
Collect data for Service Level?	Set to **y** to collect data about Service Level thresholds for reports and graphs. The default is n.
Threshold - Maximum Service Level calls	Specify the maximum number of calls that can experience a Service Level event before an event is raised. The default is 100 calls. A Service Level event occurs when one of three things happens to a call: • It is answered within the Service Level threshold. • It is abandoned within the Service Level threshold. • It reaches the Service Level threshold without being answered or abandoned.
Event severity when Service Level calls exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of Service Level calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for Service Level calls?	Set to **y** to collect data about Service Level calls for reports and graphs. The default is n.
Threshold - Maximum call-delay time	Specify the maximum number of seconds that a call can wait to be answered before an event is raised. The default is 45 seconds.
Event severity when call delay exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which call delay time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for call delay time?	Set to **y** to collect data about call delay time for reports and graphs. The default is n.
Threshold - Maximum hold time	Specify the maximum number of seconds that a call can wait on hold before an event is raised. The default is 200 seconds.
Event severity when hold time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which hold time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.

Parameter	How To Set It
Collect data for hold time?	Set to **y** to collect data about hold time for reports and graphs. The default is n.

ICM_RoutingClientData

Use this Knowledge Script to monitor data from the Routing_Client_Five_Minute table in the UCCE database. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for each routing client.

Resource Object

CISCOICM_CentralDB

Default Schedule

By default, this script runs every five minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 10 minutes. **Note** Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.

Parameter	How To Set It
On subsequent runs, query database for extended time range?	Select **Yes** to search the database beginning with records that have timestamps that fall within a time range based on twice the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:15 through 9:45. In other words, the query searches 30 minutes' worth of records beginning 60 minutes (twice the Schedule) prior to the time the job runs. Disable this option to search the database beginning with records that have timestamps that fall within a time range that is the same as the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:45 through 10:15. In other words, the query searches the most recent 30 minutes' worth of records. **Important** Select the option appropriate for your UCCE environment. In newer versions of UCCE, records are not inserted in the database until 30 minutes after the timestamp. Therefore, a record with a timestamp of 9:00 is not inserted into the database until 9:30. This Knowledge Script queries for records that have timestamps that fall within the time frame of the query. To capture records that undergo a 30-minute delay between timestamp and database insertion, select **Yes**.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum errors	Specify the maximum number of errors that can occur before an event is raised. The default is 30 errors.
Event severity when errors exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of errors exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for errors?	Set to **y** to collect data about errors for reports and graphs. The default is n.
Threshold - Maximum timed-out calls	Specify the maximum number of calls that can timeout before an event is raised. The default is five calls.
Event severity when timed-out calls exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of timed-out calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for timed-out calls?	Set to **y** to collect data about timed-out calls for reports and graphs. The default is n.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The default is 100 milliseconds.
Event severity when delay exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which delay exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for maximum delay?	Set to **y** to collect data about maximum delay for reports and graphs. The default is n.
Threshold - Maximum discarded calls	Specify the maximum number of calls that can be discarded before an event is raised. The default is 5 calls.

Parameter	How To Set It
Event severity when discarded calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of discarded calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for discarded calls	Set to **y** to collect data about discarded calls for reports and graphs. The default is n.

ICM_ScheduledTargetDataLocal

Use this Knowledge Script to monitor data from the Scheduled_Target_Real_Time table in the UCCE local database. This script raises an event if a threshold is exceeded. In addition, this script generates a separate data stream for each scheduled target. All data values reflect the current real-time value.

Resource Object

CISCOICM_LocalDB

Default Schedule

By default, this script runs every five minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 5 minutes. **Note** Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum calls in progress	Specify the maximum number of calls that can be in progress before an event is raised. The default is 100 calls.
Event severity when in-progress calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-progress calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Threshold - Minimum calls in progress	Enter the minimum number of calls that can be in progress before an event is raised. The default is 1 call.
Event severity when in-progress calls fall below the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-progress calls falls below the threshold. Set to **0** if you want to ignore the event. The default is 20.

Parameter	How To Set It
Collect data for calls in progress?	Set to **y** to collect data about in-progress calls for reports and graphs. The default is n.
Threshold - Maximum queued router calls	Specify the maximum number of router calls that can be in queue before an event is raised. The default is 20 calls.
Event severity when queued router calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of queued router calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 28.
Collect data for queued router calls?	Set to **y** to collect data about queued router calls for reports and graphs. The default is n.

ICM_ScriptData

Use this Knowledge Script to monitor data from the Script_Five_Minute table in the UCCE database. This script raises an event if a threshold is exceeded. In addition, this script generates a separate data stream for each script.

Resource Object

CISCOICM_CentralDB

Default Schedule

By default, this script runs every five minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 10 minutes. **Note** Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.

Parameter	How To Set It
On subsequent runs, query database for extended time range?	Select **Yes** to search the database beginning with records that have timestamps that fall within a time range based on twice the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:15 through 9:45. In other words, the query searches 30 minutes' worth of records beginning 60 minutes (twice the Schedule) prior to the time the job runs. Disable this option to search the database beginning with records that have timestamps that fall within a time range that is the same as the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:45 through 10:15. In other words, the query searches the most recent 30 minutes' worth of records. **Important** Select the option appropriate for your UCCE environment. In newer versions of UCCE, records are not inserted in the database until 30 minutes after the timestamp. Therefore, a record with a timestamp of 9:00 is not inserted into the database until 9:30. This Knowledge Script queries for records that have timestamps that fall within the time frame of the query. To capture records that undergo a 30-minute delay between timestamp and database insertion, select **Yes**.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum incoming calls	Specify the maximum number of calls that can be incoming before an event is raised. The default is 100 calls.
Event severity when incoming calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of incoming calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for incoming calls?	Set to **y** to collect data about incoming calls for reports and graphs. The default is n.
Threshold - Maximum routed calls	Specify the maximum number of calls that can be routed before an event is raised. The default is 100 calls.
Event severity when routed calls exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event. Set to **0** if you want to ignore the event. The default is 20.
Collect data for routed calls?	Set to **y** to collect data about routed calls for reports and graphs. The default is n.

ICM_ServiceData

Use this Knowledge Script to monitor data from the Service_Half_Hour table in the UCCE database. This script raises an event if a threshold is exceeded. In addition, this script generates a separate data stream for each service.

Resource Object

CISCOICM_CentralDB

Default Schedule

By default, this script runs every 30 minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will either the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 60 minutes. **Note** Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.

Parameter	How To Set It
On subsequent runs, query database for extended time range?	Select **Yes** to search the database beginning with records that have timestamps that fall within a time range based on twice the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:15 through 9:45. In other words, the query searches 30 minutes' worth of records beginning 60 minutes (twice the Schedule) prior to the time the job runs. Disable this option to search the database beginning with records that have timestamps that fall within a time range that is the same as the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:45 through 10:15. In other words, the query searches the most recent 30 minutes' worth of records. **Important** Select the option appropriate for your UCCE environment. In newer versions of UCCE, records are not inserted in the database until 30 minutes after the timestamp. Therefore, a record with a timestamp of 9:00 is not inserted into the database until 9:30. This Knowledge Script queries for records that have timestamps that fall within the time frame of the query. To capture records that undergo a 30-minute delay between timestamp and database insertion, select **Yes**.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum outgoing calls	Specify the maximum number of calls that can be outgoing before an event is raised. The default is 25 calls.
Event severity when outgoing calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of outgoing calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for outgoing calls?	Set to **y** to collect data about outgoing calls for reports and graphs. The default is n.
Threshold - Maximum incoming calls	Specify the maximum number of calls that can be incoming before an event is raised. The default is 100 calls.
Event severity when incoming calls exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of incoming calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for incoming calls?	Set to **y** to collect data about incoming calls for reports and graphs. The default is n.
Threshold - Maximum handled calls	Specify the maximum number of calls that can be handled before an event is raised. The default is 100 calls.
Event severity when handled calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of handled calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for handled calls?	Set to **y** to collect data about handled calls for reports and graphs. The default is n.
Threshold - Maximum abandoned calls	Specify the maximum number of calls that can be abandoned before an event is raised. The default is 5 calls.

Parameter	How To Set It
Event severity when abandoned calls exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of abandoned calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for abandoned calls?	Set to **y** to collect data about abandoned calls for reports and graphs. The default is n.
Threshold - Maximum terminated calls	Specify the maximum number of calls that can be terminated before an event is raised. The default is 5 calls.
Event severity when terminated calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of terminated calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for terminated calls?	Set to **y** to collect data about terminated calls for reports and graphs. The default is n.
Threshold - Maximum average delay	Specify the maximum amount of average delay that can occur before an event is raised. The default is 15 milliseconds.
Event severity when average delay exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of average delay exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for average delay?	Set to **y** to collect data about average delay for reports and graphs. The default is n.
Threshold - Maximum average handling time	Specify the maximum average handling time that can occur before an event is raised. The default is 100 seconds.
Event severity when average handling time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average handling time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for average handling time?	Set to **y** to collect data about average handling time for reports and graphs. The default is n.
Threshold - Maximum call delay time	Specify the longest call delay time that can occur before an event is raised. The default is 30 seconds.
Event severity when call delay time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which call delay time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for call delay time?	Set to **y** to collect data about call delay time for reports and graphs. The default is n.
Threshold - Maximum hold time	Specify the maximum amount of hold time that can occur before an event is raised. The default is 15 seconds.
Event severity when hold time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of hold time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for hold time?	Set to **y** to collect data about hold time for reports and graphs. The default is n.

ICM_ServiceDataLocal

Use this Knowledge Script to monitor data from the Service_Real_Time table in the UCCE local database. This script raises an event if a threshold is exceeded. In addition, this script generates a separate data stream for each service. All data values reflect the current real-time value.

Resource Object

CISCOICM_LocalDB

Default Schedule

By default, this script runs every five minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 5 minutes. **Note** Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum outgoing calls	Specify the maximum number of calls that can be outgoing before an event is raised. The default is 25 calls.
Event severity when outgoing calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of outgoing calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for outgoing calls?	Set to **y** to collect data about outgoing calls for reports and graphs. The default is n.
Threshold - Maximum incoming calls	Specify the maximum number of calls that can be incoming before an event is raised. The default is 100 calls.

Parameter	How To Set It
Event severity when incoming calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of incoming calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for incoming calls?	Set to **y** to collect data about incoming calls for reports and graphs. The default is n.
Threshold - Maximum handled calls	Specify the maximum number of calls that can be handled before an event is raised. The default is 100 calls.
Event severity when handled calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of handled calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for handled calls?	Set to **y** to collect data about handled calls for reports and graphs. The default is n.
Threshold - Maximum abandoned calls	Specify the maximum number of calls that can be abandoned before an event is raised. The default is 5 calls.
Event severity when abandoned calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of abandoned calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for abandoned calls?	Set to **y** to collect data about abandoned calls for reports and graphs. The default is n.
Threshold - Maximum terminated calls	Specify the maximum number of calls that can be terminated before an event is raised. The default is 5 calls.
Event severity when terminated calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of terminated calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for terminated calls?	Set to **y** to collect data about terminated calls for reports and graphs. The default is n.
Threshold - Maximum average delay	Specify the highest amount of average delay that can occur before an event is raised. The default is 15 milliseconds.
Event severity when average delay exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average delay exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for average delay?	Set to **y** to collect data about average delay for reports and graphs. The default is n.
Threshold - Maximum average handling time	Specify the highest amount of average handling time that can occur before an event is raised. The default is 100 seconds.
Event severity when average handling time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average handling time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for average handling time?	Set to **y** to collect data about handling time for reports and graphs. The default is n.
Threshold - Maximum call delay time	Specify the highest amount of call delay time that can occur before an event is raised. The default is 30 seconds.
Event severity when call delay time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which call delay time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for call delay time?	Set to **y** to collect data about call delay time for reports and graphs. The default is n.

Parameter	How To Set It
Threshold - Maximum hold time	Specify the highest amount of hold time that can occur before an event is raised. The default is 15 minutes.
Event severity when hold time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which hold time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for hold time?	Set to **y** to collect data about hold time for reports and graphs. The default is n.

ICM_SkillGroupData

Use this Knowledge Script to monitor data from the Skill_Group_Five_Minute table in the UCCE database. This script raises an event if a threshold is exceeded. Configure thresholds for five-minute intervals regardless of how often the script runs. This script generates a separate data stream for each skill group.

Resource Object

CISCOICM_CentralDB

Default Schedule

By default, this script runs every five minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will query the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 10 minutes. **Note** Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.

Parameter	How To Set It
On subsequent runs, query database for extended time range?	Select **Yes** to search the database beginning with records that have timestamps that fall within a time range based on twice the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:15 through 9:45. In other words, the query searches 30 minutes' worth of records beginning 60 minutes (twice the Schedule) prior to the time the job runs. Disable this option to search the database beginning with records that have timestamps that fall within a time range that is the same as the length of the schedule you set on the Schedule tab. For example, if you set the schedule to run every 30 minutes and the job runs at 10:15, the query searches database records with timestamps of 9:45 through 10:15. In other words, the query searches the most recent 30 minutes' worth of records. **Important** Select the option appropriate for your UCCE environment. In newer versions of UCCE, records are not inserted in the database until 30 minutes after the timestamp. Therefore, a record with a timestamp of 9:00 is not inserted into the database until 9:30. This Knowledge Script queries for records that have timestamps that fall within the time frame of the query. To capture records that undergo a 30-minute delay between timestamp and database insertion, select **Yes**.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum agents logged on	Specify the maximum number of agents that can be logged on before an event is raised. The default is 100 agents.
Event severity when logged-on agents exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of logged-on agents exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Threshold - Minimum agents logged on	Specify the minimum number of agents that can be logged on before an event is raised. The default is 1 agent.
Event severity when logged-on agents falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of logged-on agents falls below the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for logged-on agents?	Set to **y** to collect data about logged-on agents for reports and graphs. The default is n.
Threshold - Maximum time in Available state	Specify the maximum amount of time that agents can be in the Available state before an event is raised. The default is 20 seconds.
Event severity when time in Available state exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which time in the Available state exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for time in Available state?	Set to **y** to collect data about Available state time for reports and graphs. The default is n.
Threshold - Maximum time in Not Ready state	Specify the maximum amount of time that agents can be in the Not Ready state before an event is raised. The default is 20.

Parameter	How To Set It
Event severity when time in Not Ready state exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which time in the Not Ready state exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for time in Not Ready state?	Set to **y** to collect data about agents in Not Ready state for reports and graphs. The default is n.
Threshold - Maximum time in Talking state	Specify the maximum amount of time that agents can be in the Talking state before an event is raised. The default is 20 seconds.
Event severity when time in Talking state exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which time in the Talking state exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for time in Talking state?	Set to **y** to collect data about agents in Talking state for reports and graphs. The default is n.
Threshold - Maximum handled calls	Specify the maximum number of calls that can be handled before an event is raised. The default is 100 calls.
Event severity when handled calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of handled calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for handled calls?	Set to **y** to collect data about handled calls or reports and graphs. The default is n.
Threshold - Maximum average handling time	Specify the maximum amount of average handling time that can occur before an event is raised. The default is 30 seconds.
Event severity when average handling time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average handling time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for average handling time?	Set to **y** to collect data about average handling time for reports and graphs. The default is n.

ICM_SkillGroupDataLocal

Run this Knowledge Script to monitor data from the Skill_Group_Real_Time table in the UCCE local database. This script raises an event if a threshold is exceeded. In addition, this script generates a separate data stream for each skill group. All data values reflect the current real-time value.

Resource Object

CISCOICM_LocalDB

Default Schedule

By default, this script runs every five minutes.

This script is tied to a corresponding table in the SQL Server database on the UCCE server. UCCE writes data into this table at specified intervals. With this interval in mind, the default schedule for this script is set so as to gather data in real time. If you change the schedule, to either less or more frequently than the default, you will either the database more often than is necessary, or not often enough.

You should not change the default schedule for this script.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
On first run, minutes to go back	Specify the number of minutes of previous activity through which the script will search the database. For instance, if you enter 15, the script will search through the last 15 minutes of activity. The default is 5 minutes. **Note** Using a "minutes to go back" time that is larger than the default may cause this script to be CPU-intensive on its first run depending upon the number of database entries being retrieved from the UCCE server.
Cisco ICM database username	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. Leave this parameter blank in order to use Windows authentication. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Threshold - Maximum agents logged on	Specify the maximum number of agents that can be logged on before an event is raised. The default is 100 agents.
Event severity when logged-on agents exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of logged-on agents exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for logged-on agents?	Set to **y** to collect data about logged-on agents for reports and graphs. The default is n.
Threshold - Maximum time in Available state	Specify the maximum amount of time that agents can be in Available state before an event is raised. The default is 20 seconds.

Parameter	How To Set It
Event severity when time in Available state exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which time in Available state exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for time in Available state?	Set to **y** to collect data about agents in Available state for reports and graphs. The default is n.
Threshold - Maximum time in Not Ready state	Specify the maximum amount of time that agents can be in the Not Ready state before an event is raised. The default is 20 seconds.
Event severity when time in Not Ready state exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which time in Not Ready state exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for time in Not Ready state?	Set to **y** to collect data about agents in Not Ready state for reports and graphs. The default is n.
Threshold - Maximum time in Talking state	Specify the maximum amount of time that agents can be in Talking state before an event is raised. The default is 20.
Event severity when time in Talking state exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which time in Talking state exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for time in Talking state?	Set to **y** to collect data about agents in Talking state for reports and graphs. The default is n.
Threshold - Maximum handled calls	Specify the maximum number of calls that can be handled before an event is raised. The default is 100 calls.
Event severity when handled calls exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of handled calls exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for handled calls?	Set to **y** to collect data about handled calls for reports and graphs. The default is n.
Threshold - Maximum average handling time	Specify the maximum amount of average handling time that can occur before an event is raised. The default is 30 seconds.
Event severity when average handling time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average handling time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for average handling time?	Set to **y** to collect data about average handling time for reports and graphs. The default is n.
Threshold - Maximum hold time	Specify the maximum amount of hold time that can occur before an event is raised. The default is 15 seconds.
Event severity when hold time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which hold time exceeds the threshold. Set to **0** if you want to ignore the event. The default is 20.
Collect data for hold time?	Set to **y** to collect data about hold time for reports and graphs. The default is n.

IIS_CpuHigh

Use this Knowledge Script to monitor CPU usage for IIS application processes. This script raises an event if the threshold is exceeded. In addition, this script generates data streams for CPU usage (%).

Resource Object

CISCOICM_IIST_Server

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if CPU usage exceeds the threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about CPU usage for reports and graphs. The default is n.
Process names	Enter the name of the application processes to monitor. Separate multiple entries with commas. For example: `inetinfo,dllhost`. The default is inetinfo. **Note** Do not append .exe to the process names.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU resources the selected process can use before an event is raised. The default is 60%.
Event severity when CPU usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 8.

IIS_HealthCheck

Use this Knowledge Script to check IIS servers, Web site status, and the queue length for blocked I/O requests. This script raises an event if any server or Web site is not running. In addition, you can choose to automatically restart the IIS server or Web site. This script also raises an event if the blocked I/O queue length is longer than the specified threshold.

This script monitors only Web sites (servers), not FTP sites, NNTP sites, or SMTP sites.

Resource Objects

CISCOICM_IIST_Server

CISCOICM_IIST_FTPSRV

CISCOICM_IIST_W3SRV

CISCOICM_IIST_WebInst

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Auto-start monitored server(s)?	Set to **y** to automatically restart down servers. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager has not been set to restart the service. The default is 18.
Event severity for blocked I/O requests	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of blocked I/O requests exceeds the threshold. The default is 5.
Threshold - Maximum blocked I/O requests	Specify the maximum queue length for blocked I/O requests. The default is 0 requests.
Monitor IIS server?	Set to **y** to monitor the IIS server. The default is y.
Monitor FTP server?	Set to **y** to monitor the FTP server. The default is n.

IIS_KillTopCPUProcs

Use this Knowledge Script to monitor the CPU usage for the IIS `dllhost` and `mtx` processes. This script raises an event if one or both processes exceed the CPU usage threshold you set. You can set this script to automatically stop a process that exceeds the CPU usage threshold.

Resource Object

CISCOICM_IIST_Server

Default Schedule

By default, this script runs every three minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if kill is successful or unsuccessful?	Set to **y** to raise an event if the stop is successful or unsuccessful. The default is y.
Kill CPU intensive processes?	Set to **y** to automatically stop any process whose CPU usage exceeds the threshold. The default is n.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU usage allowed by the `dllhost` and `mtx` processes before an event is raised. The default is 90%.
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 10.
Event severity when kill fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the process. The default is 10.
Event severity when kill succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stopped the service. The default is 20.

IIS_MemoryHigh

Use this Knowledge Script to detect whether an IIS application process has exceeded the memory usage threshold you set. This script raises an event if an application process exceeds the memory usage threshold you set. In addition, this script generates a data stream for memory usage (%).

Resource Object

CISCOICM_IIST_Server

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, this script returns the named process's memory usage. The default is n.
Process names	Specify the name of the application process to monitor. Use a comma to separate multiple entries — do not use spaces. For example: `inetinfo,dllhost`. The default is inetinfo. **Note** Do not append .exe to the process names.
Threshold - Maximum memory usage	Specify the maximum amount of memory the selected process can use before an event is raised. The default is 10000000 bytes.
Threshold - Maximum memory pool usage	Specify the maximum amount of memory pool the selected process can use before an event is raised. The default is 5000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.

IIS_RestartServer

Use this Knowledge Script to restart an IIS server. This script raises an event if the server either successfully restarts or fails to restart.

Resource Object

CISCOICM_IIST_Server

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Restart server?	Set to **y** to automatically restart a down server. The default is y.
Wait N seconds before restarting	Specify the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the stop attempt fails. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the restart attempt fails. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the service is unavailable. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the stop attempt succeeds. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the restart attempt succeeds. The default is 25.

IIS_ServiceUpTime

Use this Knowledge Script to monitor the uptime for Web sites and services. This script raises an event if the amount of time the sites and services are running is less than the threshold you set. In addition, this script generates data streams for uptime.

Prerequisite

The computers on which you run this script must be running IIS version 5 or later.

Resource Objects

CISCOICM_IIST_WebInst

CISCOICM_IIST_FTPInst

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if uptime falls below threshold?	Set to **y** to raise an event if Web site or service uptime falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data about uptime for reports and graphs. The default is n.
Threshold - Minimum uptime	Specify the minimum amount of time that discovered Web sites and services and FTP sites and services must be up to prevent an event from being raised. The default is 10000 seconds.
Event severity when uptime falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which uptime falls below the threshold. The default is 5.

Router_AgentsLoggedOn

Use this Knowledge Script to monitor the total number of agents logged on to a Call Router. This script raises an event if the number of agents exceeds the threshold. In addition, this script generates data streams for the number of logged-on agents.

Resource Object

CISCOICM_Router

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of logged-on agents exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about logged-on agents for reports and graphs. The default is n.
Threshold - Maximum agents logged on	Specify the maximum number of agents that can be logged on before an event is raised. The default is 10 agents.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

Router_CallsInProgress

Use this Knowledge Script to monitor the number of calls in progress for a Call Router. This script raises an event if the number of calls exceeds the threshold. In addition, this script generates data streams for in-progress calls.

Resource Object

CISCOICM_Router

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of in-progress calls exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about in-progress calls for reports and graphs. The default is n.
Threshold - Maximum calls in progress	Specify the maximum number of calls that can be in progress before an event is raised. The default is 10 calls.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

Router_CallsPerSec

Use this Knowledge Script to monitor the number of in-progress calls per second for a Call Router. This script raises an event if the number of calls exceeds the threshold. In addition, this script generates data streams for per-second calls.

Resource Object

CISCOICM_Router

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of calls per second exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about per-second calls for reports and graphs. The default is n.
Threshold - Maximum in-progress calls per second	Specify the maximum number of in-progress calls that can occur per second before an event is raised. The default is 10 calls.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

SQL_Accessibility

Use this Knowledge Script to monitor SQL Server and database accessibility. This script raises an event if a SQL Server or a specified database is not accessible. In addition, this script generates data streams for database accessibility.

Resource Object

CISCOICM_SQLT_Server

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, this script returns 100 if all specified databases are accessible, 50 if some of the specified databases are accessible and some are not, or 0 if none of the specified databases is accessible. The default is y.
SQL login	Provide the database user login account that you want to use to access SQL Server. The user name you enter must have permission to access the database names for which you want to check accessibility. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Database name	Specify the database names you want to check access to, separated by commas. For example, enter `master,pubs,tempdb`. If you leave this field blank, the script checks access to all databases. The default is master.
Time out	Specify a timeout period in seconds. The timeout period is the number of seconds to wait for a response before retrying or determining the database is inaccessible. The default is 0 seconds. **Note** Keep in mind when specifying a time out that the script continues waiting until it receives a response or the timeout is reached. During this waiting period, other jobs are blocked from execution. Therefore, you should limit your use of this parameter or keep the timeout period at a minimum for regular monitoring jobs. When you are running this script to troubleshoot a particular problem and not a regularly scheduled interval for ongoing maintenance, you may want to adjust this parameter to allow a longer timeout period.

Parameter	How To Set It
Number of retries	Specify the number of times to retry connecting to the database before determining the database is inaccessible. The default is 0 retries. **Note** Keep in mind when specifying this parameter that the script continues waiting until it receives a response or has made the specified number of retry attempts. During this waiting period, other jobs are blocked from execution. Therefore, you should limit your use of this parameter or keep retry attempts at a minimum for regular monitoring jobs. When you run this script to troubleshoot a particular problem and not a regularly scheduled interval for ongoing maintenance, you may want to adjust this parameter to allow more retry attempts.
Event severity when SQL Server or database is inaccessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which SQL Server or the database is inaccessible. The default is 5.

SQL_CPUUtil

Use this Knowledge Script to monitor the percentage of CPU resources used by the `sqlservr` and `sqlagent` processes. This script raises an event if CPU usage exceeds the threshold you set. In addition, this script generates data streams for CPU usage (%).

Resource Object

CISCOICM_SQLT_Server

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if CPU usage exceeds the threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about CPU usage for reports and graphs. The default is n.
Event severity when CPU usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 8.
Monitor the SQL Server process?	Set to **y** to monitor SQL Server. The default is y.
Threshold - Maximum CPU usage for SQL Server process	Specify the maximum amount of CPU resources that can be consumed by the SQL process before an event is raised. The default is 10%.
Monitor the SQL Agent process?	Set to **y** to monitor SQL Agent. The default is y.
Threshold - Maximum CPU usage for SQL Agent process	Specify the maximum amount of CPU resources that can be consumed by the SQL Agent process before an event is raised. The default is 10%.

SQL_DataGrowthRate

Use this Knowledge Script to monitor the data growth and shrink rates for all SQL Server databases. Growth and shrink rates are calculated by taking the difference of the data space utilization from the current interval from the data space utilization from the last interval. This script raises an event if these rates exceed the thresholds you set. In addition, this script generates data streams for growth and shrink rates.

Resource Objects

CISCOICM_SQLT_DatabaseF

CISCOICM_SQLT_DatabaseObj

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Dynamically enumerate at each interval?	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y.
Exclude these objects	Specify the name of any object you want to exclude. You can exclude multiple objects, separated by commas with no spaces. For example: `master,model,mdb`. **Note** If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about data growth and shrink rates for reports and graphs. The default is n.
SQL login	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use. **Note** If you are monitoring SQL Server 7, use a `sysadmin` role account. Only members of the `sysadmin` role can retrieve file statistics on SQL Server 7.0.
Threshold - Maximum growth rate	Specify the maximum rate of data growth that is allowed between the last and current interval before an event is raised. The default is 25%.
Threshold - Maximum shrink rate	Specify the maximum rate of data shrinkage that is allowed between the last and current interval before an event is raised. The default is 25%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

SQL_DBGrowthRate

Use this Knowledge Script to monitor database growth and shrink rates. Growth and shrink rates are calculated by taking the difference between the database space utilization from the current interval and the database space utilization from the last interval. This script raises an event if these rates exceed the thresholds you set. In addition, this script generates data streams for growth and shrink rates.

Resource Objects

CISCOICM_SQLT_DatabaseF

CISCOICM_SQLT_DatabaseObj

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Dynamically enumerate at each interval	Set to **y** to dynamically enumerate databases at each monitoring interval. The default is y.
Exclude these objects	Specify the name of any object you want to exclude. You can exclude multiple objects, separated by commas with no spaces. For example: `master,model,mdb`. **Note** If you are not dynamically enumerating databases, ignore this parameter.
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about database growth and shrink rates for reports and graphs. The default is y.
SQL login	Provide the database user login account that you want to use to access SQL Server. You can use the sa account or other user login accounts that have been set up in the managed client's SQL Server. If you want to use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use. **Note** If you are monitoring SQL Server 7, use a `sysadmin` role account. Only members of the `sysadmin` role can retrieve file statistics on SQL Server 7.0.
Update usage	Set to **y** to have SQL Server recalculate the space usage. The default is n.
Threshold - Maximum growth rate	Specify the maximum percentage of database growth that is allowed between the last and current interval before an event is raised. The default is 25%.
Threshold - Maximum shrink rate	Specify the maximum percentage of database shrinkage that is allowed between the last and current interval before an event is raised. The default is 25%.

Parameter	How To Set It
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

SQL_MemUtil

Use this Knowledge Script to monitor the amount of memory that is used by Microsoft SQL Server processes: `sqlservr` and `sqlagent`.

If using SQL Server 7.0 or 2000, you can use this script to monitor total server memory usage, number of free buffers, and memory usage.

This script raises an event if memory usage exceeds the threshold you set. In addition, this script generates data streams for memory usage (%).

Resource Object

CISCOICM_SQLT_Server

Default Schedule

By default, this script runs every ten minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about memory usage for reports and graphs. The default is n.
Threshold - Maximum process memory usage	Specify the maximum amount of memory that can be consumed by SQL Server before an event is raised. The default is 50000000 bytes.
Threshold - Maximum number of free buffers	Specify the maximum number of buffers that can be in use before an event is raised. The default is 50 buffers.
Threshold - Maximum SQL Server memory usage	Specify the maximum amount of memory that can be in use by SQL Server and all related processes before an event is raised. The default is 30000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

SQL_RestartServer

Use this Knowledge Script to restart Microsoft SQL Server. This script raises an event if SQL Server either successfully restarts or fails to restart.

Resource Object

CISCOICM_SQLT_Server

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Wait N seconds before restarting	Enter the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the server. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart the server. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the server. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the server. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the server. The default is 25.

Recommended Knowledge Script Group

The following Knowledge Scripts are members of the CiscoICM Knowledge Script Group. You can find these scripts individually on the CiscoICM tab and in a group on the RECOMMENDED tab of the Operator Console.

- ICM_AgentData
- ICM_EventLog
- Router_AgentsLoggedOn
- Router_CallsInProgress
- SQL_DBGrowthRate

All scripts in the KSG have their parameters set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and run the CiscoICM group on a Cisco UCCE resource.

The CiscoICM KSG enables a "best practices" usage of AppManager for monitoring your Cisco UCCE environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the CiscoICM tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoICM tab are not affected.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the CiscoICM KSG and want to restore it to its original form, you can reinstall the AppManager for Cisco Intelligent Contact Management module on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\CiscoICM` directory.

Chapter 23
CiscoIPT Security Knowledge Scripts

The CiscoIPT Security category provides the following Knowledge Scripts that help ensure the security of your Cisco IP telephony environment.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
CCM_MaliciousCalls	Monitors the CallManager call detail record database for malicious calls as defined by Cisco.
CCM_MemoryConsumption	Monitors three CallManager services for continually excessive memory use: CallManager service, CTI Manager service, and RIS Data Collector Monitor service.
CCM_ServiceFailure	Detects the unexpected failure of critical CallManager services.
CCM_TransientConnects	Monitors transient connections to CallManager.
CCM_UnauthorizedCalls	Monitors the CallManager call detail record database for calls to and from unauthorized numbers.
CPUHigh	Monitors the total CPU usage on Cisco IP telephony servers.
CSA_Events	Monitors the CSA security logfile for several event types: emergency, critical, alert, error, warning, notice, and information.
CSA_HealthCheck	Monitors the status of CSA services, attempts to restart a service that is not running, and monitors CSA version levels.
Ettercap_Detect	Detects the presence of the Ettercap sniffer on a Cisco IP telephony server.
LoginFailures	Monitors for Windows login failures.
MemoryHigh	Monitors for user-specified services on Cisco IP telephony servers that continually consume excess memory.
ServiceFailure	Monitors for user-specified services that stop unexpectedly.
Symantec_Events	Monitors events that are flagged by a Symantec AntiVirus application.
Symantec_HealthCheck	Monitors the status of a Symantec AntiVirus application, attempts to restart the application if it is not running, and monitors any changes in the application's version level, virus definition, and Parent Server.
VerifyHotfix	Verifies whether specified hotfixes have been installed.

CCM_MaliciousCalls

Use this Knowledge Script to monitor the CallManager CDR (call detail record) database for malicious calls, as defined by Cisco. This script raises an event if malicious calls are detected.

Resource Object

CISCOIPTSECURITY_CALLMANAGER_PUBLISHER

Default Schedule

The default schedule is **Every minute**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MaliciousCalls job. The default is 5.
CDR database user name	Specify the user name required to access the CallManager CDR database. Leave this field blank to use Windows Authentication.
Monitor Malicious Calls	
Raise event if malicious call detected?	Set to **Yes** to raise an event if a malicious call is detected. The default is Yes.
Event severity when malicious call detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a malicious call is detected. The default is 10.

CCM_MemoryConsumption

Use this Knowledge Script to monitor for CallManager services that continually consume excess memory. This script raises an event if the memory threshold is exceeded three times in three iterations of the MemoryConsumption job.

This script monitors the memory use of three services:

- CallManager service
- CTI Manager service
- RIS Data Collector Monitor service

This script raises the events analyzed by the "Resource Consumption" forensic query in the Cisco IP Telephony Security module of NetIQ Security Manager. This query analyzes events for evidence indicating that a key resource has been consumed, possibly signifying a Denial of Service attack.

Note
This script differs from MemoryHigh in that it runs on a CallManager object, not the parent Cisco IPT Security object. In addition, this script is designed to monitor only three vital CallManager services. MemoryHigh allows you to specify the services that are monitored.

Resource Object

CISCOIPTSECURITY_CALLMANAGER

Default Schedule

The default schedule is **Every minute**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MemoryConsumption job. The default is 5.
Monitor CallManager Service Memory Usage	
Raise event if threshold is exceeded?	Set to **Yes** to raise an event if the amount of memory usage for the CallManager service exceeds the threshold that you set. The default is Yes.
Threshold - Maximum CallManager memory usage	Specify the maximum amount of memory usage that must occur three times before an event is raised. The default is 500,000 Kbytes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of memory usage for the CallManager service exceeds the threshold. The default is 5.
Data Collection	
Collect data for CallManager memory usage?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of CallManager memory used during the monitoring period.

Parameter	How to Set It
Monitor CallManager Service Non-Paged Pool	
Raise event if threshold is exceeded?	Set to **Yes** to raise an event if the amount of non-paged pool usage for the CallManager service exceeds the threshold that you set. The default is Yes.
Threshold - Maximum non-paged pool usage	Specify the maximum amount of non-paged pool usage that must occur three times before an event is raised. The default is 100,000 Kbytes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of non-paged pool usage for the CallManager service exceeds the threshold. The default is 5.
Data Collection	
Collect data for non-paged pool usage?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of CallManager non-paged pool used during the monitoring period.
Monitor CTI Manager Service Memory Usage	
Event Notification	
Raise event if threshold is exceeded?	Set to **Yes** to raise an event if the amount of memory usage for the CTI Manager service exceeds the threshold that you set. The default is Yes.
Threshold - Maximum CTI Manager memory usage	Specify the maximum amount of memory usage that must occur three times before an event is raised. The default is 1,000,000 Kbytes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of memory usage for the CTI Manager service exceeds the threshold. The default is 5.
Data Collection	
Collect data for CTI Manager memory usage?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of CTI Manager memory used during the monitoring period.
Monitor CTI Manager Service Non-Paged Pool	
Event Notification	
Raise event if threshold is exceeded?	Set to **Yes** to raise an event if the amount of non-paged pool usage for the CTI Manager service exceeds the threshold that you set. The default is Yes.
Threshold - Maximum CTI Manager non-paged pool	Specify the maximum amount of non-paged pool usage that must occur three times before an event is raised. The default is 100,000 Kbytes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of non-paged pool usage for the CTI Manager service exceeds the threshold. The default is 5.
Data Collection	
Collect data for CTI Manager non-paged pool?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of CTI Manager non-paged pool used during the monitoring period.
Monitor RIS Data Collector Monitor Service Memory Usage	
Event Notification	
Raise event if threshold is exceeded?	Set to **Yes** to raise an event if the amount of memory usage for the RIS Data Collector Monitor service exceeds the threshold that you set. The default is Yes.
Threshold - Maximum RIS Data Collector Monitor memory usage	Specify the maximum amount of memory usage that must occur three times before an event is raised. The default is 1,000,000 Kbytes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of memory usage for the RIS Data Collector Monitor service exceeds the threshold. The default is 5.

Parameter	How to Set It
Data Collection	
Collect data for RIS Data Collector Monitor memory usage?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of RIS Data Collector Monitor memory used during the monitoring period.
Monitor RIS Data Collector Monitor Service Non-Paged Pool	
Event Notification	
Raise event if threshold is exceeded?	Set to **Yes** to raise an event if the amount of non-paged pool usage for the RIS Data Collector Monitor service exceeds the threshold that you set. The default is Yes.
Threshold - Maximum RIS Data Collector Monitor non-paged pool	Specify the maximum amount of non-paged pool usage that must occur three times before an event is raised. The default is 100,000 Kbytes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of non-paged pool usage for the RIS Data Collector Monitor service exceeds the threshold. The default is 5.
Data Collection	
Collect data for RIS Data Collector Monitor non-paged pool?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of RIS Data Collector Monitor non-paged pool used during the monitoring period.

CCM_ServiceFailure

Use this Knowledge Script to detect the unexpected failure of the following critical CallManager service:

- Cisco CallManager
- Cisco Database Layer Monitor
- Cisco TFTP
- Cisco Telephony Call Dispatcher
- DC Directory Server
- Cisco CTIManager

This script raises an event if any monitored service stops unexpectedly.

This script raises the events that are analyzed by the "Service Failures" forensic query in the Cisco IP Telephony Security module of NetIQ Security Manager. This query analyzes events for evidence indicating that a critical service has failed, possibly signifying a Denial of Service attack.

Note
This script differs from ServiceFailure in that it runs on a CallManager object, not a parent Cisco IPT Security object. In addition, this script is designed to monitor only specific vital CallManager services. ServiceFailure allows you to specify the services that are monitored.

Resource Object

CISCOIPTSECURITY_CALLMANAGER

Default Schedule

The default schedule is **Asynchronous**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the ServiceFailure job. The default is 5.
Monitor CallManager Service Failures	
Raise event if service stops unexpectedly?	Set to **Yes** to raise an event if a monitored service stops unexpectedly. The default is Yes.
Event severity when service stops unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service stops unexpectedly. The default is 5.

CCM_TransientConnects

Use this Knowledge Script to monitor devices that perform transient (unauthorized) connections to CallManager. This script raises an event if transient connections were attempted.

A transient connection is one that is established and then immediately dropped before completing registration. Incomplete registration may indicate a device misconfiguration, a database error, or an unknown, perhaps illegal, device trying to attempt a connection.

Resource Object

CISCOIPTSECURITY_CALLMANAGER

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the TransientConnects job. The default is 5.
Monitor Transient Connections	
Event Notification	
Raise event if transient connections found?	Set to **Yes** to raise an event if transient connections were attempted. The default is Yes.
Event severity when transient connections found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which transient connections were attempted. The default is 5.

CCM_UnauthorizedCalls

Use this Knowledge Script to monitor the CallManager CDR (call detail record) database for calls to and from unauthorized numbers, which you specify. This script raises an event if unauthorized calls are detected.

This script raises the events that are analyzed by the "Unauthorized Calls" forensic query of the Cisco IP Telephony Security module of NetIQ Security Manager. This query analyzes events for evidence indicating that a certain type of unauthorized call may have been initiated.

Resource Object

CISCOIPTSECURITY_CALLMANAGER_PUBLISHER

Default Schedule

The default schedule is **Every minute**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the UnauthorizedCalls job. The default is 5.
CDR database user name	Specify the user name required to access the CallManager CDR database. Leave this field blank to use Windows Authentication.
Monitor Unauthorized Calls	
Phone numbers to monitor	Specify the phone number that you want to monitor. Any call to or from a specified number will be considered unauthorized. To monitor multiple numbers within a particular phone number pattern, type a single value with a wildcard. Remember to include any numbers necessary to access an outside line. For instance, to monitor: • All calls to "900" numbers, type `91900*` • All outside calls, type 9* **Note** To monitor multiple number patterns, or multiple numbers that do not fall within the same pattern, you will need to run this Knowledge Script again.
Event Notification	
Raise event if unauthorized call detected?	Set to **Yes** to raise an event if an unauthorized call is detected. The default is unchecked.
Event severity when unauthorized call detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an unauthorized call is detected. The default is 15.

CPUHigh

Use this Knowledge Script to monitor the total CPU usage on a Cisco IP telephony server. This script raises an event if the CPU threshold is exceeded three times in three iterations of the CPUHigh job.

This script raises the events analyzed by the "Resource Consumption" forensic query in the Cisco IP Telephony Security module of NetIQ Security Manager. This query analyzes events for evidence indicating that a key resource has been consumed, possibly signifying a Denial of Service attack.

Resource Object

CISCOIPTSECURITY

Default Schedule

The default schedule is **Every minute**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CPUHigh job. The default is 5.
Monitor Total CPU Usage	
Event Notification	
Raise event if threshold is exceeded?	Set to **Yes** to raise an event if the amount of CPU usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum CPU usage	Specify the maximum amount of CPU usage that must occur three times before an event is raised. The default is 80%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of CPU usage exceeds the threshold. The default is 5.
Data Collection	
Collect data for total CPU usage?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the total percentage of CPU usage for the monitoring period.

CSA_Events

Use this Knowledge Script to monitor the Cisco Security Agent (CSA) logfile for the following events:

- Emergency
- Critical
- Alert
- Error
- Warning
- Notice
- Information

This script raises an event for each instance of one or more of the event types that occur after you start the script.

This script raises the events that are analyzed by the "Actions Taken by Cisco Security Agent" forensic query in the Cisco IP Telephony Security module of NetIQ Security Manager. The query analyzes events for evidence indicating that an attack may have been blocked on a Cisco IP telephony server.

Resource Object

CISCOIPTSECURITY_CSA

Default Schedule

The default schedule is **Asynchronous**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CSA_Events job. The default is 5.
Monitor CSA Emergency Events	
Raise event if emergency event detected?	Set to **Yes** to raise an event if the CSA logfile contains an emergency event. The default is Yes.
Event severity when emergency event detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CSA logfile contains an emergency event. The default is 2.
Monitor CSA Critical Events	
Raise event if critical event detected?	Set to **Yes** to raise an event if the CSA logfile contains a critical event. The default is Yes.
Event severity when critical event detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CSA logfile contains a critical event. The default is 4.
Monitor CSA Alert Events	

Parameter	How to Set It
Raise event if alert event detected?	Set to **Yes** to raise an event if the CSA logfile contains an alert event. The default is Yes.
Event severity when alert event detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CSA logfile contains an alert event. The default is 6.
Monitor CSA Error Events	
Raise event if error event detected?	Set to **Yes** to raise an event if the CSA logfile contains an error event. The default is Yes.
Event severity when error event detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CSA logfile contains an error event. The default is 8.
Monitor CSA Warning Events	
Raise event if warning event detected?	Set to **Yes** to raise an event if the CSA logfile contains a warning event. The default is Yes.
Event severity when warning event detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CSA logfile contains a warning event. The default is 15.
Monitor CSA Notice Events	
Raise event if notice event detected?	Set to **Yes** to raise an event if the CSA logfile contains a notice event. The default is unchecked.
Event severity when notice event detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CSA logfile contains a notice event. The default is 20.
Monitor CSA Information Events	
Raise event if information event detected?	Set to **Yes** to raise an event if the CSA logfile contains an information event. The default is unchecked.
Event severity when information event detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CSA logfile contains an information event. The default is 25.

CSA_HealthCheck

Use this Knowledge Script to monitor the status of Cisco Security Agent (CSA) services, to restart any service that is not running, and to monitor any changes in the CSA version level. This script raises an event if a service has stopped, was restarted, or failed to restart, and raises an event if the CSA version level changes. In addition, this script generates data streams for service availability.

Resource Object

CISCOIPTSECURITY_CSA

Default Schedule

The default schedule is **Every minute**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CSA_HealthCheck job. The default is 5.
Monitor CSA Service State	
Event Notification	
Auto-start monitored service(s)?	Set to **Yes** to automatically restart any monitored CSA service that has stopped. The default is Yes.
Raise event if auto-start fails?	Set to **Yes** to raise an event if AppManager cannot restart a monitored service. The default is Yes.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart a monitored service. The default is 5.
Raise event if auto-start succeeds?	Set to **Yes** to raise an event if AppManager successfully restarts a monitored service. The default is Yes.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts a monitored service. The default is 25.
Raise event if service is not running?	Set to **Yes** to raise an event if a monitored service is not running. The default is Yes.
Event severity when service is not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service is not running. The default is 10.
Data Collection	
Collect data for service availability?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns data streams for service availability.
Monitor CSA Version Changes	

Parameter	How to Set It
Raise event if CSA version changes?	Set to **Yes** to raise an event if the CSA version number changes during the monitoring period. The default is Yes.
Event severity when CSA version changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CSA version number changes. The default is 15.

Ettercap_Detect

Use this Knowledge Script to detect the presence of the Ettercap sniffer on a Cisco IP telephony server. This script raises an event if Ettercap is installed and/or running.

The Ettercap sniffer can be altered to filter out all VoIP traffic on an IP telephony server. Its presence on an IP telephony server could constitute a breach of VoIP security.

Resource Object

CISCOIPTSECURITY

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Ettercap_Detect job. The default is 5.
Monitor Ettercap	
Event Notification	
Raise event if Ettercap is found?	Set to **Yes** to raise an event if the Ettercap sniffer is installed and/or running. The default is Yes.
Event severity when Ettercap is found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Ettercap sniffer is detected. The default is 5.

LoginFailures

Use this Knowledge Script to monitor for Windows login failures. This script raises an event if a login failure is detected.

Depending on how you have configured your Windows local audit policies, this script can monitor and raise events for two types of login failures:

- Category: Logon/Logoff. Event ID: 529
- Category: Account Logon. Event ID: 681

For example, say that you configured your audit policies to log both types of failures. An attempt to login fails, due either to a bad username or a bad password. Windows logs two events, one for each failure type. The LoginFailures script looks for both event types and generates an AppManager event for each one.

To configure Windows to log both types of login failures:

1. Click **Start > Settings > Control Panel > Administrative Tools > Local Security Policy**. The Local Security Settings window is displayed.
2. Expand **Local Policie**s and select **Audit Policy**. Several audit policies are displayed in the right-hand pane.
3. To log Account Logon event failures, right-click **Audit account logon events**, select **Properties**, click to check **Failures**, and then click **OK**.
4. To log Logon/Logoff event failures, right-click **Audit logon events**, select **Properties**, click to check **Failures**, and then click **OK**.

Resource Object

CISCOIPTSECURITY

Default Schedule

The default schedule is **Asynchronous**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the LoginFailures job. The default is 5.
Monitor NT Login Failures	
Event Notification	

Parameter	How to Set It
Raise event if a Windows login failure is detected?	Set to **Yes** to raise an event if the NT event log contains evidence of a Windows login failure. The default is Yes.
Event severity when a Windows login failure is detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a Windows login attempt has failed. The default is 5.

MemoryHigh

Use this Knowledge Script to monitor for services on Cisco IP telephony servers that continually consume excess memory. This script raises an event if the threshold is exceeded.

This script raises the events analyzed by the "Resource Consumption" forensic query in the Cisco IP Telephony Security module of NetIQ Security Manager. This query analyzes events for evidence indicating that a key resource has been consumed, possibly signifying a Denial of Service attack.

Note
This script differs from CCM_MemoryConsumption in that it runs on a parent Cisco IPT Security object, not a CallManager object. In addition, this script allows you to specify the services that are monitored. CCM_MemoryConsumption is designed to monitor only three vital CallManager services.

Resource Object

CISCOIPTSECURITY

Default Schedule

The default schedule is **Every minute**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the MemoryHigh job. The default is 5.
Services to monitor	Specify the names of one or more services to monitor for memory usage. For more than one service, enter a comma-separated list of service names. Do not include any spaces between the names and the commas.
Monitor Services	
Event Notification	
Raise event if threshold is exceeded?	Set to **Yes** to raise an event if the amount of memory usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum memory usage	Specify the maximum amount of memory usage that must occur before an event is raised. The default is 80%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of memory usage exceeds the threshold. The default is 5.
Data Collection	
Collect data for memory usage?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of memory usage for the monitoring period.

ServiceFailure

Use this Knowledge Script to monitor for Windows services that stop unexpectedly. This script raises an event when any monitored service has stopped.

This script raises the events that are analyzed by the "Service Failures" forensic query in the Cisco IP Telephony Security module of NetIQ Security Manager. This query analyzes events for evidence indicating that a critical service has failed, possibly signifying a Denial of Service attack.

Note
This script differs from CCM_ServiceFailure in that it runs on a parent Cisco IPT Security object, not a CallManager object. In addition, this script allows you to specify the services that are monitored. CCM_ServiceFailure is designed to monitor only specific vital CallManager services.

Resource Object

CISCOIPTSECURITY

Default Schedule

The default schedule is **Asynchronous**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the ServiceFailure job. The default is 5.
Services to monitor	Specify the names of one or more Windows services to monitor for unexpected stoppage. For more than one service, enter a comma-separated list of service names. Do not include any spaces between the names and the commas.
Monitor Service Failures	
Raise event if service stops unexpectedly?	Set to **Yes** to raise an event if a monitored service has stopped. The default is Yes.
Event severity when service stops unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service has stopped. The default is 5.

Symantec_Events

Use this Knowledge Script to monitor all events that are flagged by a Symantec AntiVirus application. This script raises an event if a virus is detected, if virus behavior is detected, if scan action changes, or when a file checksum or open error is detected.

This script raises the events that are analyzed by the "Virus Attacks" forensic query in the Cisco IP Telephony Security module of NetIQ Security Manager. This query analyzes events for evidence indicating that a virus may have infected a Cisco IP telephony server.

Resource Object

CISCOIPTSECURITY_Antivirus_Symantec

Default Schedule

The default schedule is **Asynchronous**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Symantec_Events job. The default is 5.
Monitor Virus Detection	
Event Notification	
Raise event if virus detected?	Set to **Yes** to raise an event if a Symantec AntiVirus application has flagged a virus. The default is Yes.
Event severity when virus detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a Symantec AntiVirus application has flagged a virus. The default is 5.
Monitor Virus Behavior Detection	
Raise event if virus behavior detected?	Set to **Yes** to raise an event if a Symantec AntiVirus application has flagged virus behavior. The default is Yes.
Event severity when virus behavior detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a Symantec AntiVirus application has flagged virus behavior. The default is 10.
Monitor Scan Action Auto-changes	
Raise event if scan action auto-changed?	Set to **Yes** to raise an event if the action for a Symantec AntiVirus application's virus-detection scan has changed. The default is Yes.
Event severity when scan action auto-changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the action for a virus-detection scan has changed. The default is 10.
Monitor File Checksum Errors	
Raise event if file checksum error?	Set to **Yes** to raise an event if an error has occurred in a Symantec AntiVirus application's file checksum. In some cases, a change in the file's checksum value could indicate that the file is infected The default is Yes.

Parameter	How to Set It
Event severity when file checksum error	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an error has occurred in the file checksum. The default is 15.
Monitor File Open Errors	
Raise event if file open error?	Set to **Yes** to raise an event if a Symantec AntiVirus application could not open a file during a virus scan. The default is unchecked.
Event severity when file open error	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a file could not be opened during a virus scan. The default is 15.

Symantec_HealthCheck

Use this Knowledge Script to monitor the status of the following Symantec AntiVirus applications, to restart an application that is not running, and to monitor any changes in an application's version level.

- Symantec AntiVirus Client
- Symantec AntiVirus
- Symantec AntiVirus Definition Watcher
- Symantec Event Manager
- Symantec Settings Manager

This script raises an event if the application has stopped, was restarted, or failed to restart, and raises an event if the application's version level, virus definition, or Parent Server changes. In addition, this script generates data streams for application availability.

Resource Object

CISCOIPTSECURITY_Antivirus_Symantec

Default Schedule

The default schedule is **Every minute**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the Symantec_HealthCheck job. The default is 5.
Monitor Symantec Service State	
Event Notification	
Auto-start Symantec service?	Set to **Yes** to automatically restart a Symantec AntiVirus application. The default is Yes.
Raise event if auto-start fails?	Set to **Yes** to raise an event if AppManager cannot restart a Symantec AntiVirus application. The default is Yes.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart a Symantec AntiVirus application. The default is 5.
Raise event if auto-start succeeds?	Set to **Yes** to raise an event if AppManager successfully restarts a Symantec AntiVirus application. The default is Yes.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts a Symantec AntiVirus application. The default is 25.
Raise event if service is not running?	Set to **Yes** to raise an event if a Symantec AntiVirus application is not running. The default is Yes.

Parameter	How to Set It
Event severity when service is not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a Symantec AntiVirus application is not running. The default is 10.
Data Collection	
Collect data for Symantec availability?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns data streams for the availability of a Symantec AntiVirus application.
Monitor Symantec Version Changes	
Raise event if Symantec version changes?	Set to **Yes** to raise an event if the version number of a Symantec Antivirus application changes during the monitoring period. The default is Yes.
Event severity when Symantec version changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the version number changes. The default is 15.
Monitor Virus Definition Changes	
Raise event if virus definition changes?	Set to **Yes** to raise an event if the virus definition for a Symantec Antivirus application changes during the monitoring period. The default is Yes.
Event severity when virus definition changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the virus definition changes. The default is 15.
Monitor Parent Server Changes	
Raise event if Parent Server changes?	Set to **Yes** to raise an event if the Parent Server for a Symantec AntiVirus application changes during the monitoring period. The default is Yes.
Event severity when Parent Server changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Parent Server changes. The default is 15.

VerifyHotfix

Use this Knowledge Script to verify whether specified hotfixes have been installed. This script raises an event if a specified hotfix is not installed. In addition, this script generates a data stream for the number of missing hotfixes.

Note
You can use the data from this script in conjunction with the ReportAM_DetailData Knowledge Script to create a hotfix exception report that details the missing hotfix IDs.

Resource Object

CISCOIPTSECURITY

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the VerifyHotfix job. The default is 5.
Hotfix identifiers	Type a list of hotfix identifiers. Separate multiple identifiers with a comma, as shown in the following example: `KB102938,KB453728,Q089786` If you need to verify more hotfixes than is convenient to enter in this field, create a list of hotfixes in a separate file and then use the following parameter.

Full path to file with list of hotfix identifiers	Type the full path to a file on the agent computer containing a list of hotfix identifiers. The file should contain the identifiers on one or more lines:
	`KB102938`
	`KB453728`
	`Q089786,Q159263`

Monitor Hotfixes	
Event Notification	
Raise event if hotfixes are not installed?	Set to **Yes** to raise an event if a specified hotfix is not installed. The default is Yes.
Event severity when hotfixes are not installed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a specified hotfix is not installed. The default is 15.
Data Collection	
Collect data for uninstalled hotfixes?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the number of specified hotfixes that are not installed.

Chapter 24
CiscoIVR Knowledge Scripts

The CiscoIVR category provides the following Knowledge Scripts for monitoring Cisco Interactive Voice Response (IVR).

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
IIS_CpuHigh	Monitors CPU usage for IIS processes.
IIS_HealthCheck	Monitors the queue length for blocked I/O requests and the up-and-down status of IIS services and Web sites.
IIS_KillTopCPUProcs	Monitors the CPU usage of the dllhost and MTX processes. Can automatically stop a process that exceeds the threshold.
IIS_MemoryHigh	Monitors memory usage and memory pool usage for IIS application processes.
IIS_RestartServer	Restarts an IIS server.
IIS_ServiceUpTime	Monitors Web sites and Web services uptime.
IVR_CpuHigh	Monitors the CPU resource consumption for IVR processes.
IVR_EventLog	Scans the Event Log for Cisco IVR errors and status events.
IVR_HealthCheck	Monitors the status of Cisco IVR services. Can automatically restarts any service that is down.
IVR_MemoryHigh	Monitors the memory consumption for IVR processes. If a process is not found, it assumes that the process is not running, and reports zero as the memory result.
IVR_RestartService	Schedules an IVR service to stop and then restart after a specified interval.
IVR_SystemUsage	Monitors the CPU usage and memory for the Cisco IVR process and for system processes.
Report_ServicesAvailability	Summarizes the average availability of IVR services.
Report_SystemUsage	Summarizes the average CPU and memory usage per IVR server.

IIS_CpuHigh

Use this Knowledge Script to monitor CPU usage for IIS application processes. This script raises an event if CPU usage exceeds the threshold you set. In addition, this script generates data streams for CPU usage.

Resource Object

CISCOIVR_IIST_Server

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if CPU usage exceeds threshold?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data for CPU usage?	Set to **y** to collect data about CPU usage for reports and graphs. The default is n.
Process names	Specify the names of the application processes you want to monitor. Separate multiple entries with commas. For example: `inetinfo,dllhost`. The default is inetinfo. **Note** Do not append `.exe` to the process names.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU resources the selected process can use before an event is raised. The default is 60%.
Event severity when CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold you set. The default is 8.

IIS_HealthCheck

Use this Knowledge Script to check IIS servers, Web site status, and the queue length for blocked I/O requests. This script raises an event if any server or Web site is not running. In addition, you can choose to automatically restart the IIS server or Web site. This script also raises an event if the blocked I/O queue length is longer than the specified threshold.

This script monitors only Web sites (servers), not FTP sites, NNTP sites, or SMTP sites.

Resource Objects

- CISCOIVR_IIST_Server
- CISCOIVR_IIST_FTPSRV
- CISCOIVR_IIST_W3SRV
- CISCOIVR_IIST_WebInst

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Auto-start monitored server(s)?	Set to **y** to automatically restart servers that are down. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a server is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a server was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which a server is down and AppManager has not been set to restart the service. The default is 18.
Event severity for blocked I/O requests	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 5.
Threshold - Maximum blocked I/O requests	Specify the maximum queue length for blocked I/O requests. The default is 0 requests.
Monitor IIS server?	Set to **y** to monitor the IIS server. The default is y.
Monitor FTP server?	Set to **y** to monitor the FTP server. The default is n.

IIS_KillTopCPUProcs

Use this Knowledge Script to monitor the CPU usage for the IIS `dllhost` and `mtx` processes. This script raises an event if one or both processes exceed the CPU usage threshold you set. You can set this script to automatically stop a process that exceeds the CPU usage threshold.

Resource Object

CISCOIVR_IIST_Server

Default Schedule

The default schedule is **Every three minutes**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if kill is successful or unsuccessful?	Set to **y** to raise an event when a process is successfully or unsuccessfully stopped. The default is y.
Kill CPU intensive processes?	Set to **y** to automatically stop any process that exceeds the threshold. The default is n.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU that can be used by the `dllhost` and `mtx` processes before an event is raised. The default is 90%.
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold you set. The default is 10.
Event severity when kill fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop a process. The default is 10.
Event severity when kill succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops a process. The default is 20.

IIS_MemoryHigh

Use this Knowledge Script to monitor memory usage for IIS applications. This script raises an event if memory usage exceeds the threshold. In addition, this script generates data streams for memory usage.

Resource Object

CISCOIVR_IIST_Server

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if threshold is exceeded? ?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about memory usage for reports and graphs. The default is n.
Process names	Specify the names of the application processes you want to monitor. Use a comma to separate multiple entries — do not use spaces. For example: `inetinfo,dllhost`. The default is inetinfo. **Note** Do not append .exe to the process names.
Threshold - Maximum memory usage	Specify the maximum amount of memory the selected process can use before an event is raised. The default is 10000000 bytes.
Threshold - Maximum memory pool usage	Specify the maximum amount of memory pool the selected process can use before an event is raised. The default is 5000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.

IIS_RestartServer

Use this Knowledge Script to restart an IIS server. This script raises an event if the server either successfully restarts or fails to restart.

Resource Object

CISCOIVR_IIST_Server

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Wait N seconds before restarting	Specify the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the server. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart the server. The default is 5.
Event severity when status of server is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the server. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the server. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the server. The default is 25.

IIS_ServiceUpTime

Use this Knowledge Script to monitor the uptime for Web sites and services. This script raises an event if the amount of time the sites and services are running is less than the threshold you set. In addition, this script generates data streams for uptime.

Note
This script supports IIS version 5 and later.

Resource Objects

- CISCOIVR_IIST_WebInst
- CISCOIVR_IIST_FTPInst

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if uptime falls below threshold?	Set to **y** to raise an event when uptime falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, the script returns how long a service has been running. The default is n.
Threshold - Minimum uptime	Specify the minimum amount of time that discovered Web sites, Web services, FTP sites, and FTP services are required to be up during any interval to prevent an event from being raised. If the sites and services up time is less than this threshold, an event is raised. The default is 10000 seconds.
Event severity when uptime falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which uptime falls below the threshold. The default is 5.

IVR_CpuHigh

Use this Knowledge Script to monitor the CPU resource consumption for IVR processes. This script raises an event if CPU utilization exceeds the thresholds you set. The script monitors CPU usage for each IVR process and the total CPU usage for all processes. If a process is not found, the script assumes that the process is not running and reports zero as the CPU result.

Resource Object

CISCOIVR

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Threshold - Maximum CPU usage for Cisco Application/CRA/CRS Engine	Specify the maximum amount CPU that can be used by the Cisco Application/CRA/CRS Engine before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.
Threshold - Maximum CPU usage for Cisco AVVID Alarm Service	Specify the maximum CPU usage for Cisco AVVID Alarm Service that can be detected before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%
Threshold - Maximum CPU usage for Cisco Syslog Collector	Specify the maximum CPU usage for Cisco Syslog Collector that can be detected before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.

IVR_EventLog

Use this Knowledge Script to monitor the event log entries from Cisco IVR during the past *n* hours. This script raises an event if log entries are detected. In addition, this script generates datastreams for log entries.

Resource Object

CISCOIVR

Default Schedule

The default schedule is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event for log entries?	Set to **y** to raise an event when the log contains entries for which you have filtered. The default is y.
Collect data?	Set to **y** to collect data about log entries for charts and graphs. The default is n.
Separate data?	Set to **y** to separate events entries from different log files into different data streams. If set to **n**, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. The default is n. For example, if you are monitoring both the System and Application logs, you may want to set this parameter to **y** so that events in the System log are tracked separately from events in the Application log.
Log source	Specify the event log you want to monitor. Separate multiple entries by commas. For example: `System,Application`. The default is Application.
Events in past N hours	Enter the number of hours of log file entries through which the script will search for events that match the criteria you specify. For instance, if you enter 15, then the script will search through the last 15 hours of log file entries. If you enter **0**, which is the default, no past events are looked at during the first iteration of the Knowledge Script job. During subsequent iterations, the script will look through and filter only the new events that have been created in the Windows event log.
Type: Error	Set to **y** to monitor for error events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for the **Collect data?** parameter. The default is y.
Type: Warning	Set to **y** to monitor for warning events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for the **Collect data?** parameter. The default is y.

Parameter	How To Set It
Type: Information	Set to **y** to monitor for information events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for the **Collect data?** parameter. The default is n.
Type: Success Audit	Set to **y** to monitor for success audit events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for the **Collect data?** parameter. The default is n.
Type: Failure Audit	Set to **y** to monitor for failure audit events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified **y** for the **Collect data?** parameter. The default is n.
Instructions for filters: To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log. The search string can contain criteria used to include entries, exclude entries, or both.· • Separate include and exclude criteria with a colon (:). For example, `net:logon`. • Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ`. • If you are specifying only include criteria, the colon is not necessary. For example, `SQL`. • If you are specifying only exclude criteria, start the search string with a colon. For example, `:defragmentation,cleanup`.	
Event source filter	Specify one or more text strings to look for; separate multiple strings with commas. If your valid text string includes a comma, replace the comma with a tilde. For example: `Cisco Systems~ Inc. CRS` The Knowledge Script will convert the tilde to a comma at runtime.
Event category filter	Specify one or more text strings to look for; separate multiple strings with commas.
Event ID filter	Specify a single event ID or a range of event IDs; separate multiple entries by commas. For example: `1094,1404-1463`
Event user filter	Specify a single or multiple user names to look for; separate multiple entries by commas. For example: `Pat,Chris,Alex`
Computer filter	Specify a single or multiple computer names to look for; separate multiple entries by commas. For example: `SHASTA,MARS`
Event description filter	Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods; separate multiple entries with commas. For example: `data loss during system failures,corrupt indices,Inter-Site Transport objects failed`

Parameter	How To Set It
Threshold - Maximum number of entries per event report	Specify the maximum number of Application log events that can be returned in each event report. For example, if this value is set to 30 and 67 Application log events are found, then three event reports are raised: two reports containing 30 events and one report containing seven events. The default is 30. The Message column on the **Events** tab in the Operator Console displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.
Event severity for log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event in which log entries are detected. You may want to adjust the severity depending on the types of events for which you are checking. The default is 15.

IVR_HealthCheck

Use this Knowledge Script to monitor Cisco IVR services. This script raises an event if any service is not running, and can automatically re-start any service that is not running. To make the most of the data collected by this script, run Report_ServicesAvailability.

Resource Object

CISCOIVR

Default Schedule

The default schedule is **Every minute**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Collect data?	Set to **y** to collect data for reports and graphs. The default is y.
Auto-start monitored services?	Set to **y** to auto-start any of the services that you choose to monitor. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager has not been set to restart the service. The default is 18.
Event severity when service does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service does not exist. The default is 15.
Monitor the Cisco Application/CRA/CRS Engine service?	Set to **y** to monitor the Cisco Application/CRA/CRS Engine service. The default is y.
Monitor the Cisco AVVID Alarm service?	Set to **y** to monitor the Cisco AVVID Alarm service. The default is y.
Monitor the Cisco Syslog Collector service?	Set to **y** to monitor the Cisco Syslog Collector service. The default is n.

IVR_MemoryHigh

Use this Knowledge Script to monitor the memory consumption for IVR processes. This script checks the memory used by each IVR process individually, and the total memory used by all processes. If a process is not found, the script assumes that the process is not running, and reports zero as the memory result.

This script raises an event if any value exceeds the threshold you set.

Resource Object

CISCOIVR

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Monitor Cisco Application/CRA/CRS Engine memory usage?	Set to **y** to monitor the memory usage of the Cisco Application/CRA/CRS Engine. The default is y.
Threshold - Maximum memory usage for Cisco Application/CRA/CRS Engine	Specify the maximum amount of memory that can be used by the Cisco Application/CRA/CRS Engine before an event is raised. The default is 200000 KB.
Threshold - Maximum memory pool usage for Cisco Application/CRA/CRS Engine	Specify the maximum amount of memory pool that can be used by the Cisco Application/CRA/CRS Engine before an event is raised. The default is 5000 KB.
Monitor Cisco AVVID Alarm Service memory usage?	Set to **y** to monitor the memory usage of Cisco AVVID Alarm Service. The default is y.
Threshold - Maximum memory usage for Cisco AVVID Alarm Service	Specify the maximum amount of memory that can be used by the Cisco AVVID Alarm Service before an event is raised. The default is 200000 KB.
Threshold - Maximum memory pool usage for Cisco AVVID Alarm Service	Specify the maximum amount of memory pool that can be used by the Cisco AVVID Alarm Service before an event is raised. The default is 5000 KB.
Monitor Cisco Syslog Collector memory usage?	Set to **y** to monitor the memory usage of Cisco Syslog Collector. The default is y.
Threshold - Maximum memory usage for Cisco Syslog Collector	Specify the maximum amount of memory that can be used by the Cisco Syslog Collector before an event is raised. The default is 200000 KB.
Threshold - Maximum memory pool usage for Cisco Syslog Collector	Specify the maximum amount of memory pool that can be used by the Cisco Syslog Collector before an event is raised. The default is 5000 KB.

IVR_RestartService

Use this Knowledge Script to schedule an IVR service to stop and then restart after a specified interval. This script raises an event when a stop or restart fails, when service status is unavailable, and when a stop or restart succeeds.

Resource Object

CISCOIVR

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Collect data?	Set to **y** to collect data for graphs and reports. The default is n.
Wait N seconds before restarting	Specify the number of seconds that should elapse before the service is restarted. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the service. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart the service. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the service. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the service. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the service. The default is 25.
Restart Cisco Application/CRA/CRS Engine service?	Set to **y** to restart the Cisco Application/CRA/CRS Engine. The default is y.
Restart Cisco AVVID Alarm service?	Set to **y** to restart the Cisco AVVID Alarm. The default is n.
Restart Cisco Syslog Collector service?	Set to **y** to restart the Cisco Syslog Collector. The default is n.

IVR_SystemUsage

Use this Knowledge Script to monitor CPU usage and memory for the Cisco IVR process. This script raises an event if a threshold is exceeded. To make the most of the data collected by this script, run Report_SystemUsage.

Resource Object

CISCOIVR

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is y.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Threshold - Maximum IVR server CPU usage	Specify the maximum amount of IVR CPU that can be in use before an event is raised. The default is 75%.
Threshold - Maximum total CPU usage	Specify the maximum amount of total CPU that can be in use before an event is raised. The default is 90%.
Threshold - Maximum IVR server memory usage	Specify the maximum amount of IVR memory that can be in use before an event is raised. The default is 75%.
Threshold - Maximum total memory usage	Specify the maximum amount of total memory that can be in use before an event is raised. The default is 90%.

Report_ServicesAvailability

Use this Knowledge Script to summarize the average availability of each IVR service within a time frame that you specify. This script uses the data collected by the IVR_HealthCheck script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Data Source	
Select data wizard	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the Knowledge Scripts that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Decimal accuracy for % values	Specify the number of decimal places that you want to see in the values displayed in this report. The default is 3.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CiscoIVRServicesAvailability.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set the report properties as desired. The default report name is Cisco IVR Services Availability.

Parameter	How To Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report is successful?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_SystemUsage

Use this Knowledge Script to summarize the average CPU and memory usage per IVR server within a time frame that you specify. This script uses the data collected by the IVR_SystemUsage script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Data Source	
Select data wizard	Select the computers that you want to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the Knowledge Scripts that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Charts	
Include % CPU chart?	Set to **y** to include a chart that details the CPU usage for the selected cluster. The default is y.
Include memory usage chart?	Set to **y** to include a chart that details the memory usage for the selected cluster. The default is y.
% CPU chart threshold	Specify the CPU percentage threshold to display on the charts in the report. The default is 0%.
Memory usage chart threshold	Specify the physical memory threshold to display on the charts in the report. The default is 0 KB.
Chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Chart color scheme	Select a color scheme template. The default is NetIQ1.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of information in the report. The default is y.
Select output folder	Locate and select the output folder. The default folder name is CiscoIVRSystemUsage.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.

Parameter	How To Set It
Select properties	Set the report properties as desired. The default report name is Cisco IVR System Usage.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report is successful?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event when the report is successful. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Chapter 25
CiscoUnity Knowledge Scripts

AppManager Knowledge Scripts can help you better manage Cisco Unity resources. From within the Operator Console, you can select a Knowledge Script in the CiscoUnity tab of the Knowledge Script pane and press **F1** for complete details.

Knowledge Script	What It Does
CU_BackupAndRestoreStatus	Monitors the success or failure of the Cisco Disaster Recovery Tool (DiRT) Backup and Restore utility.
CU_CallActivity	Monitors the number of incoming and outgoing calls to the Unity server during an interval you specify.
CU_CpuHigh	Monitors the CPU resource consumption for Unity processes.
CU_CurrentDiskQueueLength	Monitors the number of requests outstanding on the disk.
CU_EventLog	Scans the Event Log for Cisco Unity errors and status events.
CU_FailoverStatus	Monitors whether failover or failback has occurred on the current server.
CU_HealthCheck	Monitors the status of Cisco Unity services. Can automatically restart any service that is down.
CU_LicenseCompliance	Monitors the number of Unified Messaging and/or Voice Mail licences and determines how many of those licenses are actively used.
CU_MemoryHigh	Monitors the memory consumption for Unity processes.
CU_MessageDeliveryFailure	Determines whether errors prohibited the Unity Message Repository (UMR) or the Message Transfer Agent (MTA) from successfully delivering all messages.
CU_MessageStoreAvailability	Monitors the number of offline message stores.
CU_MessageStoreLock	Monitors the number of tics it takes to acquire a Message Store Lock.
CU_NumberOfLogons	Monitors the number of active logons to Cisco Unity.
CU_PortStatus	Monitors whether a Unity port is unavailable and unable to handle further calls.
CU_ProcessorQueueLength	Monitors the number of processes in queue for the Processor.
CU_RestartService	Schedules a Unity service to stop and then restart after a specified interval.
CU_Silence	Monitors all of the silence performance counters for the Unity Manager Service in tenths of a second.
CU_SystemUsage	Monitors the CPU usage and memory for the Cisco Unity Manager process and for system processes.
CU_TTSPortsInUse	Monitors the number of text-to-speech ports being used by callers.

Knowledge Script	What It Does
CU_UMRServiceHung	Determines whether the AvUMRSyncSvr service is hung. This script is supported only for Cisco Unity version 3.0(x).
CU_VoicePortsInUse	Determines the number of voice ports currently in use on the Unity server.
IIS_CpuHigh	Monitors CPU usage for IIS processes.
IIS_HealthCheck	Monitors the queue length for blocked I/O requests and the up-and-down status of IIS services and Web sites.
IIS_KillTopCPUProcs	Monitors the CPU usage of the dllhost and MTX processes. Can automatically stop a process that exceeds the threshold.
IIS_MemoryHigh	Monitors memory usage and memory pool usage for IIS application processes.
IIS_RestartServer	Restarts an IIS server.
IIS_ServiceUpTime	Monitors Web sites and the uptime for Web services.
Report_PortUsage	Summarizes the number of Unity ports in use. This script uses the data collected by the CU_TTSPortsInUse and CU_VoicePortsInUse scripts.
Report_ServicesAvailability	Summarizes the average availability of Unity services.
Report_SystemUsage	Summarizes average CPU and memory usage per Unity server.
SQL_Accessibility	Monitors whether the SQL Server database is accessible.
SQL_CPUUtil	Monitors CPU usage for SQL Server processes.
SQL_DataGrowthRate	Monitors data growth and shrink rates for all SQL Server databases.
SQL_DBGrowthRate	Monitors database growth and shrink rates.
SQL_MemUtil	Monitors memory usage for SQL Server processes.
SQL_RestartServer	Restarts a SQL Server.
Recommended Knowledge Script Groups	Performs essential monitoring of your Cisco Unity environment.
Discovery_CiscoUnity	Discovers Cisco Unity resources and configuration information.

CU_BackupAndRestoreStatus

Use this Knowledge Script to monitor the success or failure of the Cisco Disaster Recovery Tool (DiRT) Backup and Restore utility.

You use the DiRT utility to back up Cisco Unity-specific data — including SQL databases, registry settings, greetings, recorded names, switch file configuration, routing rules, and subscriber passwords — and then restore the information onto the Cisco Unity unified messaging server.

This script raises an event if backup/restore succeeds or fails. In addition, this script generates data streams for successful backup/restore operations.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data for successful backup/ restore?	Set to **y** to collect data about a successful backup and restore. The default is n.
Raise event if backup/restore succeeds?	Set to **y** to raise an event when a backup or restore is successful. The default is y.
Event severity if backup/restore succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a backup or restore is successful. The default is 25.
Raise event if backup/restore fails?	Set to **y** to raise an event when a backup or restore fails. The default is y.
Event severity if backup/restore fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a backup or restore fails. The default is 5.

CU_CallActivity

Use this Knowledge Script to monitor incoming and outgoing calls to the Unity server. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for number and percentage of incoming calls, number and percentage of outgoing calls, number and percentage per second of incoming calls, and number and percentage per second of outgoing calls.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to **y** to collect data about incoming and outgoing calls for graphs and reports. The default is y.
Threshold type	Select whether you want to set a threshold based on a **Percentage** or a **Value**. The default is Percentage.
Monitor incoming calls?	Set to **y** to monitor incoming calls. The default is y.
Threshold - Maximum percentage of incoming calls	Specify the highest percentage of incoming calls that can occur before an event is raised. The default is 80%.
Threshold - Maximum number of incoming calls	Specify the highest number of incoming calls that can occur before an event is raised. The default is 18 calls.
Event severity if incoming calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage or number of incoming calls exceeds the threshold. The default is 15.
Monitor outgoing calls?	Set to **y** to monitor outgoing calls. The default is y.
Threshold - Maximum percentage of outgoing calls	Specify the highest percentage of outgoing calls that can occur before an event is raised. The default is 80%.
Threshold - Maximum number of outgoing calls	Specify the highest number of outgoing calls that can occur before an event is raised. The default is 18 calls.
Event severity if outgoing calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage or number of outgoing calls exceeds the threshold. The default is 15.
Monitor incoming calls per second?	Set to **y** to monitor incoming calls per second. The default is y.
Threshold - Maximum percentage of incoming calls per second	Specify the highest percentage of incoming calls that can occur per second before an event is raised. The default is 80%.
Threshold - Maximum number of incoming calls per second	Specify the highest number of incoming calls that can occur per second before an event is raised. The default is 18 calls.
Event severity if incoming calls per second exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage or number of incoming calls per second exceeds the threshold. The default is 15.

Parameter	How to Set It
Monitor outgoing calls per second?	Set to **y** to monitor outgoing calls per second. The default is y.
Threshold for percentage of outgoing calls per second	Specify the highest percentage of outgoing calls that can occur per second before an event is raised. The default is 80%.
Threshold for number of outgoing calls per second	Specify the highest number of outgoing calls that can occur per second before an event is raised. The default is 18 calls.
Event severity for outgoing calls per second	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage or number of incoming calls per second exceeds the threshold. The default is 15.

CU_CpuHigh

Use this Knowledge Script to monitor CPU usage for the following Unity processes:

- Unity Manager
- Secure Gateway
- Message Repository
- Directory Change Writer
- Active Directory Datastore
- Global Catalog Datastore
- Event Reporter
- Report Handler
- Exchange 5.5 Datastore
- Text-To-Speech
- Bridge Connector
- AvLic
- AvMMProxySvr
- AvMsgStoreMonitorSvr
- AvNotifierMgr
- AvSqlChangeWriter

This script raises an event if CPU usage exceeds the thresholds you set. The script generates data streams for CPU usage for each process individually and the total CPU usage for all processes. If a process is not found, the script assumes the process is not running, and reports zero for CPU usage.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when CPU utilization exceeds threshold?	Set to **y** to raise an event when CPU usage exceeds a threshold. The default is y.
Collect data?	Set to **y** to collect data about CPU usage for graphs and charts. The default is n.

Parameter	How to Set It
Event severity when CPU utilization exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds a threshold. The default is 8.
Threshold - Maximum CPU usage for ...	Specify the maximum amount of CPU usage that must be detected before an event is raised. Set to **0** if you do not want to monitor this process. The default is for Unity Manager is 80%. The default for all other services is 20%.

CU_CurrentDiskQueueLength

Use this Knowledge Script to monitor the number of requests outstanding on the disk. This script raises an event if a threshold is exceeded. In addition, this script generates a data stream for the number of requests in queue.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if requests in queue exceed threshold?	Set to **y** to raise event an event if the number of requests in queue exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n.
Threshold - Maximum requests in queue	Specify the maximum number of requests that can be in the disk queue before an event is raised. The default is 10 requests.
Event severity if requests in queue exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of requests in queue exceeds the threshold. The default is 25.

CU_EventLog

Use this Knowledge Script to monitor the event log entries from Cisco Unity during the past *n* hours. This script raises an event when log entries are detected. In addition, this script generates data streams for those log entries.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event for log entries?	Set to **y** to raise an event when the log contains entries for which you have filtered. The default is y.
Collect data?	Set to **y** to collect data about log entries for charts and graphs. The default is n.
Separate data?	Set to **y** to separate events entries from different log files into different data streams. If set to **n**, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. The default is n. For example, if you are monitoring both the System and Application logs, you may want to set this parameter to **y** so events in the System log are tracked separately from events in the Application log.
Log source	Specify the event log you want to monitor. You can specify multiple event logs, separated by commas. For example: `System,Application`. The default is Application.
Type: Error	Set to **y** to monitor for error events. If set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the *Collect data* parameter. The default is y.
Type: Warning	Set to **y** to monitor for warning events. If set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the *Collect data* parameter. The default is y.
Type: Information	Set to **y** to monitor for information events. If set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the *Collect data* parameter. The default is n.
Type: Success Audit	Set to **y** to monitor for success audit events. If set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the *Collect data* parameter. The default is n.

Parameter	How to Set It
Type: Failure Audit	Set to **y** to monitor for failure audit events. If set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the *Collect data* parameter. The default is n.
Instructions for filtering: To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log. The search string can contain criteria used to include entries, exclude entries, or both.· • Separate include and exclude criteria with a colon (:). For example, `net:logon`. • Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ` • If you specify only include criteria, the colon is not necessary. For example, `SQL` • If you specify only exclude criteria, start the search string with a colon. For example, `:defragmentation,cleanup`	
Event source filter	Specify one or more text strings to look for; separate multiple strings with commas. For example: `NTDS KCC,NTDS General`
Event category filter	Specify one or more text strings to look for; separate multiple strings with commas.
Event ID filter	Specify a single event ID or a range of event IDs; separate multiple entries by commas. For example: `1094,1404-1463`
Event user filter	Specify a single or multiple user names to look for; separate multiple entries by commas. For example: `Pat,Chris,Alex`
Computer filter	Specify a single or multiple computer names to look for; separate multiple entries by commas. For example: `SHASTA,MARS`
Event description filter	Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods; separate multiple entries with commas. For example: `data loss during system failures,corrupt indices,Inter-Site Transport objects failed`
Maximum number of entries per event report	Specify the maximum number of Application log events that can be returned in each event report. For example, if this value is set to 30 and 67 Application log events are found, then three event reports are raised: two reports containing 30 events and one report containing seven events. The default is 30. The Message column on the Events tab in the Operator Console displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.
Event severity for log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the log contains entries for which you have filtered. You may want to adjust the severity depending on the types of events for which you are checking. The default is 8.

CU_FailoverStatus

Use this Knowledge Script to determine whether failover or failback has occurred on the current server. The first time you run this script on a particular server, you can choose to raise an informational event indicating whether the current computer is the active computer. The word "Primary" or "Secondary" accompany each computer name in the event.

- **Failover**. A feature that provides simple redundancy, allowing voice messaging functions to continue if the Cisco Unity server fails or when you need to perform maintenance. A primary and secondary Unity server (failover pair) allow for continuous voice messaging functionality. When the status of the primary server changes from active to inactive, the secondary server takes over the tasks of the primary server.
- **Failback.** A feature that allows the secondary Unity server to shutdown down its functionality and allows the primary Unity server to take back the ability to answer calls.
- **Primary Unity server**. As the primary server of a failover pair, this server replicates all the appropriate Unity data to its backup counterpart (the secondary).
- **Secondary Unity server**. This server is basically an identical copy of the primary Unity server. The secondary server takes over for the primary server in the event of a failover.
- **AvCsNodeMgr.exe**. The Unity service responsible for determining whether failover or failback needs (or is scheduled) to occur.

The failover feature of Cisco Unity provides simple redundancy, allowing voice messaging functions to continue if the Cisco Unity server fails or when you need to perform maintenance. A primary and secondary Unity server (failover pair) allow for continuous voice messaging functionality. When the status of the primary server changes from active to inactive, the secondary server takes over the tasks of the primary server.

Use this script to monitor the status of failover and failback, which occurs when the primary server resumes its tasks.

To create a failover pair, set the *Create failover pair server group* parameter in the Discovery_CiscoUnity Knowledge Script to **y**. An Action Knowledge Script — AddComputerToServerGroup — runs by default and creates a server group composed of the two computers on which you run the Discovery script.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every minute.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when failover occurs?	Set to **y** to raise an event when failover occurs. A failover event message will indicate which computer is now the primary computer in the failover scenario. In addition, the event will indicate when the next failback is schedule to occur. The event indicates if failback is not scheduled. The default is y.
Event severity when failover occurs	Set the severity level, from 1 to 40, to indicate the importance of a failover event. The default is 15.
Raise event when failback occurs?	Set to **y** to raise an event when failback occurs. A failback event message will indicate which computer is now the primary computer in the failback scenario. The default is y.
Event severity when failback occurs	Set the severity level, from 1 to 40, to indicate the importance of a failback event. The default is 15.
Raise event for initial failover configuration and status?	Set to **y** to raise an informational event indicating the current configuration — Primary or Secondary — and status — active or inactive — of the Unity server. The default is y.
Collect data?	Set to **y** to collect data about failover status values (1 for active and 0 for inactive) for graphs and reports. The default is n.

CU_HealthCheck

Use this Knowledge Script to monitor the status of the following Cisco Unity services:

- Unity Manager
- Secure Gateway
- Message Repository
- Directory Change Writer
- Active Directory Store
- Global Catalog Datastore
- Event Reporter
- Report Handler
- Exchange 5.5 Datastore
- Text-To-Speech
- Bridge Connector
- Node Manager
- Licensing
- Media Master Proxy Server
- Message Store Monitor
- Notifier
- SQL Change Writer

This script raises an event if any service is not running. In addition, this script can automatically restart any service that is not running, as well as generate data streams for service status.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every minute.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to **y** to collect data about service status for charts and graphs. The default is y.
Auto-start the monitored services?	Set to **y** to auto-start the services you choose to monitor. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which auto-start fails. The default is 5.

Parameter	How to Set It
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which auto-start succeeds. The default is 25.
Event severity when auto-start is set to “n”	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager has not been set to restart the service. The default is 5.
Event severity when service doesn’t exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service does not exist. The default is 25.
Monitor ..... service?	Set to **y** to monitor Unity services. The default for Unity Manager is y. The default for all other services is n.

CU_LicenseCompliance

Use this Knowledge Script to monitor the number of Unified Messaging and/or Voice Mail licences and determine how many of those licenses are actively used. This script raises an event a threshold is exceeded. In addition, this script generates data streams for number and percentage of licenses used.

Note
This script supports Cisco Unity version 4.0(3) and later.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every 24 hours.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data for licenses used?	Set to **y** to collect data about in-use licenses for reports and graphs. The default is n.
Threshold type	Select the type of threshold you want to set. Select **Percentage** to set a threshold for a percentage of in-use licenses. Select **Value** to set a threshold for a number of in-use licenses. The default is Percentage.
Threshold - Maximum percentage of licenses used	Specify the threshold for the highest percentage of licenses that can be in use before an event is raised. The default is 80%.
Threshold - Maximum number of licenses used	Specify the threshold for the highest number of licenses that can be in use before an event is raised. The default is 24 licenses.
Event severity if used licenses exceed threshold	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number or percentage of in-use licenses exceeds the threshold you set. The default is 15.

CU_MemoryHigh

Use this Knowledge Script to monitor memory usage for the following Unity processes:

- Unity Manager
- Secure Gateway
- Message Repository
- Directory Change Writer
- Active Directory Datastore
- Global Catalog Datastore
- Event Reporter
- Exchange 5.5 Datastore
- Text-To-Speech
- Bridge Connector
- Licensing Service
- Media Master Proxy Server
- Message Store Monitor
- Notifier
- SQL Change Writer

This script checks the memory used by each process individually and the total memory used by all processes. If a process is not found, the script assumes the process is not running, and reports zero as the memory result.

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for memory usage for all monitored applications.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when threshold exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.

Parameter	How to Set It
Monitor Unity Manager memory usage?	Set to **y** to monitor the memory usage of Unity Manager. The default is y.
Threshold - Maximum memory usage for Unity Manager	Specify the maximum memory usage that can occur before an event is raised. The default is 200000 KB.
Threshold - Maximum memory pool usage for Unity Manager	Specify the maximum memory pool usage that can occur before an event is raised. The default is 5000 KB.
Monitor Secure Gateway memory usage	Set to **y** to monitor the memory usage of Secure Gateway. The default is y.
Threshold - Maximum memory usage for Secure Gateway	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Secure Gateway	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Message Repository memory usage?	Set to **y** to monitor the memory usage of Message Repository. The default is y.
Threshold - Maximum memory usage for Message Repository	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Message Repository	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Directory Change Writer memory usage?	Set to **y** to monitor the memory usage of Directory Change Writer. The default is y.
Threshold - Maximum memory usage for Directory Change Writer	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Directory Change Writer	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Active Directory Datastore memory usage?	Set to **y** to monitor the memory usage of Active Directory Datastore. The default is y.
Threshold - Maximum memory usage for Active Directory Datastore	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Active Directory Datastore	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Global Catalog Datastore memory usage?	Set to **y** to monitor the memory usage of Global Catalog Datastore. The default is y.
Threshold - Maximum memory usage for Global Catalog Datastore	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Global Catalog Datastore	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Event Reporter memory usage?	Set to **y** to monitor the memory usage of Event Reporter. The default is y.
Threshold - Maximum memory usage for Event Reporter	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Event Reporter	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Report Handler memory usage?	Set to **y** to monitor the memory usage of Report Handler. The default is y.
Threshold - Maximum memory usage for Report Handler	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.

Parameter	How to Set It
Threshold - Maximum memory pool usage for Report Handler	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Exchange 5.5 Datastore memory usage?	Set to **y** to monitor the memory usage of Exchange 5.5 Datastore. The default is y.
Threshold - Maximum memory usage for Exchange 5.5 Datastore	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Exchange 5.5 Datastore	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Text-To-Speech memory usage?	Set to **y** to monitor the memory usage of Text-To-Speech. The default is y.
Threshold - Maximum memory usage for Text-To-Speech	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Text-To-Speech	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Bridge Connector memory usage?	Set to **y** to monitor the memory usage of the Bridge Connector. The default is y.
Threshold - Maximum memory usage for Bridge Connector	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Bridge Connector	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Licensing Service memory usage?	Set to **y** to monitor the memory usage of the Licensing Service. The default is y.
Threshold - Maximum memory usage for the Licensing Service	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for the Licensing Service	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Media Master Proxy Server memory usage?	Set to **y** to monitor the memory usage of the Media Master Proxy Server. The default is y.
Threshold - Maximum memory usage for the Media Master Proxy Server	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB
Threshold - Maximum memory pool usage for the Media Master Proxy Server	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Message Store Monitor memory usage?	Set to **y** to monitor the memory usage of the Message Store Monitor. The default is y.
Threshold - Maximum memory usage for the Message Store Monitor	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB
Threshold - Maximum memory pool usage for the Message Store Monitor	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor Notifier memory usage?	Set to **y** to monitor the memory usage of the Notifier. The default is y.
Threshold - Maximum memory usage for the Notifier	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB
Threshold - Maximum memory pool usage for the Notifier	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.
Monitor SQL Change Writer memory usage?	Set to **y** to monitor the memory usage of the SQL Change Writer. The default is y.

Parameter	How to Set It
Threshold - Maximum memory usage for the SQL Change Writer	Specify the maximum memory usage that can occur before an event is raised. The default is 100000 KB
Threshold - Maximum memory pool usage for the SQL Change Writer	Specify the maximum memory pool usage that can occur before an event is raised. The default is 2500 KB.

CU_MessageDeliveryFailure

Use this Knowledge Script to determine whether errors prohibited the Unity Message Repository (UMR) or the Message Transfer Agent (MTA) from successfully delivering all messages. Messages not delivered successfully are stored locally on the Unity server. You can set this script to retrieve a count of the messages that are in storage awaiting delivery.

This script raises an event if messages are not delivered successfully. In addition, this script generates data streams for the number of unsuccessful deliveries for UMR and MTA.

Note
This script replaces CU_MTAFailures, which has been removed from the CiscoUnity category of Knowledge Scripts.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if MTA failure prevents message delivery	Set to **Yes** to raise an event if MTA messages are not delivered. The default is Yes.
Event severity if MTA failure prevents message delivery	Set the event notification level, from 1 to 40, to indicate the importance of an event in which MTA messages are not delivered. The default is 10.
Raise event if UMR failure prevents message delivery	Set to **Yes** to raise an event if UMR messages are not delivered. The default is Yes.
Event severity if UMR failure prevents message delivery	Set the event notification level, from 1 to 40, to indicate the importance of an event in which UMR messages are not delivered. The default is 10.
Data Collection	
Collect data for failed message deliveries due to MTA failure?	Set to **Yes** to collect data about undelivered MTA messages for reports and graphs.
Collect data for failed message deliveries due to UMR failure?	Set to **Yes** to collect data about undelivered UMR messages for reports and graphs.

CU_MessageStoreAvailability

Use this Knowledge Script to monitor the number of offline message stores. This script raises an event if a message store goes offline. In addition, this script generates data streams for the number of offline message stores.

Note
This script supports Cisco Unity versions 4.0(3) and later.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every 600 seconds.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MessageStoreAvailability job fails. The default is 5.
Monitor Message Store Availability	
Event Notification	
Raise event if message store goes offline?	Set to **Yes** to raise an event if a message store goes offline. The default is Yes.
Event severity when message store goes offline	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a message store goes offline. The default is 5.
Data Collection	
Collect data for number of offline message stores?	Set to **Yes** to collect data about offline message store for reports and graphs. The default is unchecked.

CU_MessageStoreLock

Use this Knowledge Script to monitor the number of tics it takes to acquire a Message Store Lock. This script raises an event a threshold is exceeded. In addition, this script generates data streams for number of tics.

Note
This script does not support Cisco Unity versions 4.0(3) and later.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when number of tics exceeds threshold?	Set to **y** to raise event if the number of tics required to acquire a Message Store Lock exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about tics for charts and graphs. The default is n.
Threshold - Maximum number of tics to acquire a Message Store Lock	Specify the maximum number of tics it takes to acquire a Message Store Lock before an event is raised. The default is 4 tics.
Event severity when number of tics exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

CU_NumberOfLogons

Use this Knowledge Script to monitor the number of active subscriber sessions to Cisco Unity. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the number of active subscriber sessions.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if active subscriber sessions exceed threshold?	Set to **y** to raise event if the number of active subscriber sessions exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data about subscriber sessions for charts and graphs. The default is n.
Threshold - Maximum number of active subscriber sessions	Specify the maximum number of subscriber sessions that can be active before an event is raised. Enter a number appropriate for the server you are monitoring. The default is 20 sessions.
Event severity when active subscriber sessions exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active subscriber sessions exceeds the threshold. The default is 25.

CU_PortStatus

Use this Knowledge Script to monitor whether a Unity port is unavailable and unable to handle further calls. This script raises an event if a port is unavailable. In addition, this script generates data streams for port availability.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if a port is unavailable?	Set to y to raise an event when a port is unavailable. The default is y.
Collect data?	Set to **y** to collect data about unavailable ports for charts and graphs. The default is n.
Event severity when a port is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which a port is unavailable. The default is 8.

CU_ProcessorQueueLength

Use this Knowledge Script to monitor the number of processes in queue for the processor. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for queue length.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if queue length exceeds threshold?	Set to **y** to raise event if the queue length exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data about queue length for charts and graphs. The default is n.
Threshold - Maximum number of processes in queue	Specify the maximum number of processes that can be in the queue before an event is raised. The default is 10 processes.
Event severity when queue length exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of processes in queue exceeds the threshold. The default is 25.

CU_RestartService

Use this Knowledge Script to schedule the following Unity services to stop and then restart after a specified interval:

- Unity Manager
- Secure Gateway
- Message Repository
- Directory Change Writer
- Active Directory Datastore
- Global Catalog Datastore
- Event Reporter
- Exchange 5.5 Datastore
- Text-To-Speech
- Bridge Connector
- Licensing Service
- Media Master Proxy Server
- Message Store Monitor
- Notifier
- SQL Change Writer

This script raises an event when a stop or restart fails, when service status is unavailable, and when a stop or restart succeeds. In addition, this script generates data streams for service status.

Note
This script does not support Cisco Unity versions 4.0(3) and later.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to **y** to collect data about service status for charts and graphs. The default is n.
Wait N seconds before restarting	Specify the number of seconds that should elapse before a service is restarted. The default is 5 seconds.

Parameter	How to Set It
Event severity when stop fails	Set the event severity level, from 1 to 40,to indicate the importance of an event in which AppManager fails to stop a service. The default is 5.
Event severity when restart fails	Set the event severity level, from 1 to 40,to indicate the importance of an event in which AppManager fails to restart a service. The default is 5.
Event severity when status of service is unavailable	Set the event severity level, from 1 to 40,to indicate the importance of an event in which service status is unavailable. The default is 10.
Event severity when stop succeeds	Set the event severity level, from 1 to 40,to indicate the importance of an event in which AppManager successfully stops a service. The default is 25.
Event severity when restart succeeds	Set the event severity level, from 1 to 40,to indicate the importance of an event in which AppManager successfully restarts a service. The default is 25.
Restart …. service?	Set to **y** to restart any of the listed Unity services. The default is n.
Unity 3.1-only Services	
Restart ... service?	Set to **y** to restart any of the listed 3.1 Unity services. The default is n.

CU_Silence

Use this Knowledge Script to monitor all of the silence performance counters for the Unity Manager Service in tenths of a second. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for silence length for all monitored performance counters.

Note
This script does not support Cisco Unity versions 4.0(3) and later.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if a counter exceeds its threshold?	Set to **y** to raise an event if any of the counters exceeds its threshold. The default is y.
Collect data?	Set to **y** to collect data about silence counters for charts and graphs. The default is n.
Threshold - Maximum time for any silence performance counter	Specify the maximum amount of time for any silence performance counter. An event is raised if the threshold is exceeded. The default is .04 seconds.
Threshold - Maximum time for Header silence	Specify the maximum amount of time for Header silence. An event is raised if the threshold is exceeded. The default is .04 seconds.
Threshold - Maximum time for Logon silence	Specify the maximum amount of time for Logon silence. An event is raised if the threshold is exceeded. The default is .04 seconds.
Threshold - Maximum time for Message Delete silence	Specify the maximum amount of time for Message Delete silence. An event is raised if the threshold is exceeded. The default is .04 seconds.
Threshold - Maximum time for Opening silence	Specify the maximum amount of time for Opening silence. An event is raised if the threshold is exceeded. The default is .04 seconds.
Threshold - Maximum time for Play Message silence	Specify the maximum amount of time for Play Message silence. An event is raised if the threshold is exceeded. The default is .04 seconds.
Threshold - Maximum time for Record silence	Specify the maximum amount of time for Record silence. An event is raised if the threshold is exceeded. The default is .04 seconds.
Event severity when a counter exceeds its threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 25.

CU_SystemUsage

Use this Knowledge Script to monitor CPU usage and memory for the Cisco Unity Process. This script raises an event if any threshold is exceeded. In addition, this script generates data streams for maximum and total CPU usage (%) and maximum and total memory usage (%).

To generate reports based on the data collected by this script, run Report_SystemUsage and Report_ServicesAvailability.

Note
On the Advanced tab, set the *Raise event if event condition occurs* parameter to 3 times within 3 job iterations to prevent the raising of events at peak usage.

Resource Object

CiscoUnity

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when threshold is exceeded?	Set to **y** to raise event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is y.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Threshold - Maximum Unity CPU usage	Specify the maximum Unity CPU usage that must occur before an event is raised. The default is 65%.
Threshold - Maximum total CPU usage	Specify the maximum total CPU usage that must occur before an event is raised. The default is 80%.
Threshold - Maximum Unity memory usage	Specify the maximum Unity memory usage that must occur before an event is raised. The default is 65%.
Threshold - Maximum total memory usage	Specify the maximum total memory usage that must occur before an event is raised. The default is 80%.

CU_TTSPortsInUse

Use this Knowledge Script to monitor the number of Cisco Unity text-to-speech (TTS) ports that are in use. This script raises an event if a threshold is exceeded. A port is considered “in use” when a Unity subscriber is having his or her email read back over the phone.

This script generates data streams for number of ports in use.

Administrators can use this script to determine whether there are sufficient TTS port licenses and to gather usage statistics.

Resource Object

CISCOUNITY_TTSPorts

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when number of in-use TTS ports exceeds threshold?	Set to **y** to raise an event when the number of ports in use exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about TTS ports for charts and graphs. The default is y. **Note** If the status of the Unity server changes from "active" to "inactive," data collection for this script will stop. Data collection will resume when status changes back to "active."
Threshold - Maximum number of TTS ports in use	Specify the maximum number of TTS ports that can be in use before an event is raised. Enter a number appropriate for the server you are monitoring. The default is 4 ports.
Event severity when number of in-use TTS ports exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-use TTS ports exceeds the threshold. The default is 5.

CU_UMRServiceHung

Use this Knowledge Script to determine whether the AvUMRSyncSvr service is unresponsive. By default, this script always raises an event if AvUMRSyncSvr is unresponsive. In addition, you can choose to raise an event if AvUMRSyncSvr is *not* unresponsive.

UMR is the Unity Message Repository.

Note
This script supports Cisco Unity version 3.0(x) only.

Resource Object

CISCOUNITY

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event when AvUMRSyncSvr service is not hung?	Set to **y** to raise an event if the AvUMRSyncSvr service is *not* unresponsive. The default is n.
Event severity when AvUMRSyncSvr service is hung	Set the severity level, from 1 to 40, to indicate the importance of an event in which the AvUMRSyncSvr service is unresponsive. The default is 8.

CU_VoicePortsInUse

Use this Knowledge Script to monitor the number of Cisco Unity voice ports that are in use. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for the number of voice ports in use.

Administrators can use this script to identify episodes of high usage, to determine whether there are sufficient voice port licenses on the Unity server, and to determine the availability of voice ports.

Resource Object

CISCOUNITY_Ports

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if in-use voice ports exceed threshold?	Set to **y** to raise an event when the number of ports in use exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about voice ports for charts and graphs. The default is y. **Note** If the status of the Unity server changes from "active" to "inactive," data collection for this script will stop. Data collection will resume when status changes back to "active."
Threshold - Maximum voice ports in use	Specify the maximum number of voice ports that can be in use before an event is raised. Enter a value appropriate for the server you are monitoring. The default is 4 ports.
Event severity when in-use voice ports exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-use voice ports exceeds the threshold. The default is 5.

IIS_CpuHigh

Use this Knowledge Script to monitor CPU usage for IIS application processes. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for CPU usage (%) for each monitored process.

Resource Object

CISCOUNITY_IIST_Server

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if CPU usage exceeds threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If enabled, data collection returns CPU usage for the specified process. The default is n.
Process names	Type the name of the processes you want to monitor. Separate multiple entries with commas. For example: `inetinfo,dllhost`. The default is inetinfo. **Note** Do not append .exe to the process names.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU usage that can occur before an event is raised. The default is 60%.
Event severity when CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 8.

IIS_HealthCheck

Use this Knowledge Script to check IIS servers, Web site status, and the queue length for blocked I/O requests. This script raises an event if any server or Web site is not running. In addition, you can choose to automatically restart the IIS server or Web site. This script also raises an event if the blocked I/O queue length is longer than the specified threshold.

Note
This script monitors only Web sites (servers), not FTP sites, NNTP sites, or SMTP sites.

Resource Objects

- CISCOUNITY_IIST_Server
- CISCOUNITY_IIST_FTPSRV
- CISCOUNITY_IIST_W3SRV
- CISCOUNITY_IIST_WebInst

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Auto-start monitored server(s)?	Set to **y** to automatically restart down servers. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which auto-start fails. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which auto-start succeeds. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager has not been set to restart the service. The default is 18.
Event severity for blocked I/O requests	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Threshold - Maximum blocked I/O requests	Specify the maximum number of blocked I/O requests that can be in the queue before an event is raised. The default is 0 requests.
Monitor IIS server?	Set to **y** to monitor the IIS server. The default is y.
Monitor FTP server?	Set to **y** to monitor the FTP server. The default is n.

IIS_KillTopCPUProcs

Use this Knowledge Script to monitor the CPU usage for the IIS `dllhost` and `mtx` processes. This script raises an event if a threshold is exceeded. In addition, this script can automatically stop a process that exceeds the CPU usage threshold.

Resource Object

CISCOUNITY_IIST_Server

Default Schedule

By default, this script runs every three minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if kill is successful or unsuccessful?	Set to **y** to raise an event if the stop process is successful or unsuccessful. The default is y.
Kill CPU-intensive processes?	Set to **y** to automatically stop any process that exceeds the CPU usage threshold. The default is n.
Threshold - Maximum CPU usage allowed	Specify the maximum percentage of CPU usage allowed by the `dllhost` and `mtx` processes before an event is raised. The default is 90%.
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 10.
Event severity when kill fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a process is exceeding the threshold and AppManager cannot stop the process. The default is 10.
Event severity when kill succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a process is exceeding the threshold and AppManager has successfully stopped the process. The default is 20.

IIS_MemoryHigh

Use this Knowledge Script to monitor the memory usage of specified processes. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for memory usage per process.

Resource Object

CISCOUNITY_IIST_Server

Default Schedule

By default, this script runs every three minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If enabled, data collection returns memory usage for the specified process. The default is n.
Process names	Enter the name of the application process to monitor. Use a comma to separate multiple entries — do not use spaces. For example: `inetinfo,dllhost`. The default is inetinfo. **Note** Do not append .exe to the process names.
Threshold - Maximum memory usage	Specify the maximum amount of memory the selected process can use before an event is raised. The default is 10000000 bytes.
Threshold - Maximum memory pool usage	Specify the maximum amount of memory pool the selected process can use before an event is raised. The default is 5000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.

IIS_RestartServer

Use this Knowledge Script to restart an IIS server. This script raises an event if the server successfully restarts or fails to restart.

Resource Object

CISCOUNITY_IIST_Server

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Restart server?	Set to **y** to automatically restart a server that is down. The default is y.
Wait N seconds before restarting	Enter the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the AppManager fails to stop the server. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager fails to restart the server. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the service is unavailable. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the server. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the server. The default is 25.

IIS_ServiceUpTime

Use this Knowledge Script to monitor the uptime for Web sites and services. This script raises an event if any value falls below the threshold. In addition, this script generates data streams for service uptime.

Note
This script runs on IIS version 5 and later.

Resource Objects

- CISCOUNITY_IIST_WebInst
- CISCOUNITY_IIST_FTPInst

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if uptime falls below threshold?	Set to **y** to raise an event if uptime falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If enabled, data collection returns the length of time a service has been running. The default is n.
Threshold - Minimum uptime	Specify the minimum number of seconds that discovered Web sites and services and FTP sites and services are required to be up to prevent an event from being raised. If up time for sites and services is less than this threshold, an event is raised. The default is 10000 seconds.
Event severity when uptime falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which uptime falls below the threshold. The default is 5.

Report_PortUsage

Use this Knowledge Script to summarize the number of Unity ports in use for a given time frame. This script uses the data collected by the CU_TTSPortsInUse and CU_VoicePortsInUse scripts.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Port type	Select the type of port for which you are running the report: TTS or Voice. The default is Voice.
Select data wizard	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the Knowledge Scripts you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekdays	Select the days of the week to include in your report. The default is Sunday through Saturday.
Aggregate by n minutes?	Specify the interval in minutes in which time-period data will be grouped. The default is 60 minutes.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of information in the report. The default is y.
Include chart?	Set to **y** to include a chart in the report. The default is y.
Select chart style	Define chart properties in the Chart Settings dialog box. The default style is Area.
Select output folder	Select the output folder. The default folder name is CiscoUnityVoicePortUsage.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set report properties as desired. The default report name is Cisco Unity Voice Port Usage.

Parameter	How to Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Event severity for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5.

Report_ServicesAvailability

Use this Knowledge Script to summarize the average availability of Unity services within a time frame you specify. This script uses the data collected by the CU_HealthCheck script.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the Knowledge Scripts you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Decimal accuracy for % values	Enter the number of decimal places you want to see in the values displayed in this report. The default is 3.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CiscoUnityServicesAvailability.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.
Select properties	Set report properties as desired. The default report name is Cisco Unity Services Availability.

Parameter	How to Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5.

Report_SystemUsage

Use this Knowledge Script to summarize the average CPU and memory usage within a time frame you specify. This script uses the data collected by the CU_SystemUsage script.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select data wizard	Select the computers you want to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the Knowledge Scripts you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Charts	
Include % CPU chart?	Set to **y** to include a chart that details the CPU usage for the selected cluster. The default is y.
Include memory usage chart?	Set to **y** to include a chart that details the memory usage for the selected cluster. The default is y.
% CPU chart threshold	Enter the CPU percentage threshold to display on the charts in the report. The default is 0%.
Memory usage chart threshold	Enter the physical memory threshold (in KB) to display on the charts in the report. The default is 0 KB.
Chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Chart color scheme	Select a color scheme template. The default is NetIQ1.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of information in the report. The default is y.
Select output folder	Locate and select the output folder. The default folder name is CiscoUnitySystemUsage.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps correlate a specific instance of a Report script with the corresponding report.

Parameter	How to Set It
Select properties	Set report properties as desired. The default report name is Cisco Unity System Usage.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5.

SQL_Accessibility

Use this Knowledge Script to monitor SQL Server and database accessibility. This script raises an event if SQL Server or a specified database is not accessible. In addition, this script generates a data stream for database accessibility.

Resource Object

CISCOUNITY_SQLT_Server

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data?	Set to **y** to collect data for reports and graphs. If enabled, data collection returns 100 if all specified databases are accessible, 50 if some of the specified databases are accessible and some are not, or 0 if none of the specified databases is accessible. The default is n.
SQL login	Type the database username that provides access SQL Server. The username must have permission to access the database names for which you want to check accessibility. To use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use.
Database name	Type the names of the databases to which you want to check access, separated by commas. For example, type `master,pubs,tempdb`. If you leave this field blank, the script checks access to all databases. The default is master.
Timeout	Specify the number of seconds to wait for a response before retrying or determining the database is inaccessible. The default is 0 seconds. **Note** Keep in mind the Knowledge Script continues waiting until it receives a response or the timeout is reached. During this waiting period, other jobs are blocked from execution. Therefore, you should limit your use of this parameter or keep the time out period at a minimum for regular monitoring jobs. If you run this script to troubleshoot a particular problem and not as part of a regularly scheduled interval for ongoing maintenance, you may want to adjust this parameter to allow a longer time out period.

Parameter	How to Set It
Number of retries	Specify the number of times to retry connecting to the database before determining the database is inaccessible. The default is 0 retries. **Note** Keep in mind the script continues waiting until it receives a response or has made the specified number of retry attempts. During this waiting period, other jobs are blocked from execution. Therefore, you should limit your use of this parameter or keep retry attempts at a minimum for regular monitoring jobs. If you run this script to troubleshoot a particular problem and not as part of a regularly scheduled interval for ongoing maintenance, you may want to adjust this parameter to allow more retry attempts.
Event severity if SQL Server or database inaccessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which SQL Server or the database is not accessible. The default is 5.

SQL_CPUUtil

Use this Knowledge Script to monitor the percentage of CPU resources used by the `sqlservr` and `sqlagent` processes. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for CPU usage (%) for all monitored processes.

Resource Object

CISCOUNITY_SQLT_Server

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if CPU usage exceeds threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If enabled, data collection returns information about the CPU resources used by SQL processes. The default is n.
Event severity when CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 8.
Monitor the SQL Server process?	Set to **y** to monitor SQL Server. The default is y.
Threshold - Maximum CPU usage for SQL Server process	Specify the maximum amount of CPU resources that can be consumed by the SQL Server process before an event is raised. The default is 10%.
Monitor the SQL Agent process?	Set to **y** to monitor SQL Agent. The default is y.
Threshold - Maximum CPU usage for SQL Agent process	Specify the maximum amount of CPU resources that can be consumed by the SQL Agent process before an event is raised. The default is 10%.

SQL_DataGrowthRate

Use this Knowledge Script to monitor the data growth and shrink rates for all SQL Server databases. Growth and shrink rates are calculated by taking the difference of the data space utilization from the current interval from the data space utilization from the last interval. This script raises an event if growth and shrink rates exceed the thresholds you set. In addition, this script generates data streams for data growth and shrink rates for each monitored database.

Resource Objects

- CISCOUNITY_SQLT_DatabaseF
- CISCOUNITY_SQLT_DatabaseObj

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to **y** to automatically count databases at each monitoring interval. The default is y.
Exclude these objects	Type the name of any object you want to exclude. You can exclude multiple objects, separated by commas with no spaces. For example, enter `master,model,mdb` **Note** Ignore this parameter if you are not dynamically enumerating databases.
Raise event if threshold exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If enabled, data collection returns the data growth and shrink rates for each database. The default is n.
SQL login	Enter the database username that provides access to SQL Server. You can use the "sa" account or other user login account that has been set up in the managed client's SQL Server. To use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use. **Note** If you are monitoring SQL Server 7, use a `sysadmin` role account. Only members of the `sysadmin` role can retrieve file statistics on SQL Server 7.0.
Threshold - Maximum growth rate	Specify the maximum percentage of data growth allowed between the last and current interval before an event is raised. Enter **0** to ignore this parameter. The default is 25%.
Threshold - Maximum shrink rate	Specify the maximum percentage of data shrinkage allowed between the last and current interval before an event is raised. Enter **0** to ignore this parameter. The default is 25%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

SQL_DBGrowthRate

Use this Knowledge Script to monitor database growth and shrink rates. Growth and shrink rates are calculated by taking the difference between the database space utilization from the current interval and the database space utilization from the last interval. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for database growth and shrink rates.

Resource Objects

- CISCOUNITY_SQLT_DatabaseF
- CISCOUNITY_SQLT_DatabaseObj

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Dynamically enumerate at each interval	Set to **y** to automatically count databases at each monitoring interval. The default is y.
Exclude these objects	Enter the name of any object you want to exclude. You can exclude multiple objects, separated by commas with no spaces. For example, enter `master,model,mdb` **Note** Ignore this parameter if you are not dynamically enumerating databases.
Raise event if threshold exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If enabled, data collection returns database growth and shrink rates. The default is y.
SQL login	Enter the database username that provides access to SQL Server. You can use the "sa" account or other user login account that has been set up in the managed client's SQL Server. To use a specific SQL Server login account, use AppManager Security Manager to update the AppManager repository with the SQL Server logins you want to use. **Note** If you are monitoring SQL Server 7, use a `sysadmin` role account. Only members of the `sysadmin` role can retrieve file statistics on SQL Server 7.0.
Update usage?	Set to **y** to have SQL Server recalculate the space usage. The default is n.
Threshold - Maximum growth rate	Enter the maximum percentage of data growth allowed between the last and current interval before an event is raised. Enter **0** to ignore this parameter. The default is 25%.

Parameter	How to Set It
Threshold - Maximum shrink rate	Enter the maximum percentage of data shrinkage allowed between the last and current interval before an event is raised. Enter **0** to ignore this parameter. The default is 25%.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

SQL_MemUtil

Use this Knowledge Script to monitor the amount of memory used by SQL Server processes. This script monitors the `sqlservr` and `sqlagent` processes.

If using SQL Server 7.0 or 2000, you can use this script to monitor total server memory usage, number of free buffers, and memory usage.

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for memory usage for SQL Server processes.

Resource Object

CISCOUNITY_SQLT_Server

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If enabled, data collection returns information about the amount of memory used by SQL Server. The default is n.
Threshold - Maximum process memory usage	Specify the maximum amount of memory that can be consumed by SQL Server before an event is raised. The default is 50000000 bytes.
Threshold - Maximum number of free buffers	Specify the maximum number of buffers that can be in use before an event is raised. The default is 50 buffers.
Threshold - Maximum SQL Server memory usage	Specify the maximum amount of memory that can be in use by SQL Server and all related processes before an event is raised. The default is 30000000 bytes.
Event severity when threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

SQL_RestartServer

Use this Knowledge Script to restart SQL Server. This script raises an event if the server successfully restarts or fails to restart. In order to restart SQL services, this script will also stop dependent Unity services, such as `AvCsMgr` and `AvUMRSyncSvr`. This script automatically restarts any service that it stops.

Resource Object

CISCOUNITY_SQLT_Server

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Wait N seconds before restarting	Enter the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the server. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart the server. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the server. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the server. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the server. The default is 25.

Recommended Knowledge Script Groups

The following Knowledge Scripts are members of the CiscoUnity recommended Knowledge Script Group. You can find these scripts individually on the CiscoUnity tab and in a group on the RECOMMENDED tab of the Operator Console.

- CU_HealthCheck
- CU_NumberOfLogons
- CU_Silence
- CU_SystemUsage
- CU_VoicePortsInUse

The following scripts are members of the CiscoUnity_Reports recommended KSG:

- Report_PortUsage.
- Report_ServicesAvailability.
- Report_SystemUsage.

All scripts in the KSGs have their parameters set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and run the KSG on a Cisco Unity or Report resource.

The KSGs enable a “best practices” usage of AppManager for monitoring your Cisco Unity environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView.

A KSG is composed of a subset of a module’s Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the CiscoUnity tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoUnity tab are not affected.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the CiscoUnity or CiscoUnity_Report KSG and want to restore it to its original form, you can reinstall AppManager for Cisco Unity on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\CiscoUnity` directory.

Discovery_CiscoUnity

Use this Knowledge Script to discover Cisco Unity resources, including the TSP version, and ports.

Resource Object

NT_MachineFolder

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when discovery succeeds?	This script always raises an event when the discovery fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discover fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery partially succeeds. The default is 15.
SQL username	If appropriate, enter your SQL username. Leave this field blank to use Windows Authentication. **Note** If a SQL username is required, then you must configure the user name into AppManager Security Manager.
Create failover pair server group?	Set to **y** to create a server group composed of a failover pair (primary and secondary Unity servers). This server group is visible in the TreeView pane from the Master view only. The default is y.

Chapter 26
CiscoUnityBridge Knowledge Scripts

The CiscoUnityBridge category provides the following Knowledge Scripts for monitoring Unity Bridge servers.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
CUB_CpuHigh	Monitors the CPU resources that application processes are consuming.
CUB_EventLog	Monitors the event log entries from Unity Bridge during the past *n* hours.
CUB_HealthCheck	Monitors the status of Unity Bridge services. Can automatically restarts any service that is down.
CUB_MemoryHigh	Monitors the memory that application processes are consuming. If a process is not found, it assumes that the process is not running, and reports zero as the memory result.
CUB_RestartService	Schedules a Unity Bridge service to stop and then restart after a specified interval.
CUB_SystemUsage	Monitors CPU usage and memory for the Unity Bridge process and for system processes.
IIS_CpuHigh	Monitors CPU usage for IIS processes.
IIS_HealthCheck	Monitors the queue length for blocked I/O requests and the up-and-down status of IIS services and Web sites.
IIS_KillTopCPUProcs	Monitors CPU usage for the IIS `dllhost` and `mtx` processes. Can automatically stop a process that exceeds the CPU usage threshold.
IIS_MemoryHigh	Monitors memory usage and memory pool usage for IIS application processes.
IIS_RestartServer	Restarts an IIS server.
IIS_ServiceUpTime	Monitors the uptime of Web sites and Web services.
Report_ServicesAvail	Summarize the average availability of Unity Bridge-related services.
Report_SystemUsage	Summarizes the average CPU and memory usage per Unity Bridge server.

CUB_CpuHigh

Use this Knowledge Script to monitor the CPU resources that the Unity Bridge and Digital Networking processes are consuming. This script raises an event if CPU utilization exceeds the thresholds you set. The script monitors CPU usage for each process individually and the total CPU usage for all processes. If a process is not found, the script assumes that the process is not running, and reports zero as the CPU result.

Resource Object

CISCOUNITYBRIDGE

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Raise event if threshold exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data for CPU usage?	Set to **y** to collect data about CPU usage for graphs and reports. The default is n.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.
Threshold - Maximum CPU usage for Unity Bridge	Specify the highest percentage of CPU usage by the Unity Bridge process that must occur before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.
Threshold - Maximum CPU usage for Digital Networking	Specify the highest percentage of CPU usage by the Digital Networking process that must occur before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.

CUB_EventLog

Use this Knowledge Script to monitor the event log entries from Cisco Unity Bridge during the past *n* hours. This script raises an event if log entries are detected. In addition, this script generates data streams for log entries.

Resource Object

CISCOUNITYBRIDGE

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Raise event for log entries?	Set to **y** to raise an event when the log contains entries for which you have filtered. The default is y.
Collect data?	Set to **y** to collect data about log entries for graphs and reports. The default is n.
Separate data?	Set to **y** to separate events entries from different log files into different data streams. If set to **n**, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. The default is n. For example, if you are monitoring both the System and Application logs, you may want to set this parameter to **y** so that events in the System log are tracked separately from events in the Application log.
Log source	Specify the event log you want to monitor. You can specify multiple event logs, separated by commas. For example: `System,Application`. The default is Application.
Events in past N hours	Set this parameter to determine which events are searched for the first time the script is run. Subsequent searches begin where the last search finished. The following entries are valid: • Enter -1 to search all current and previous Directory Service log events during the first interval. • Accept the default of 0 to search only for current events; previous events are not searched. • Enter the number of hours to go back in the Directory Service log to scan for matching events. For example, enter 8 to scan the last eight hours of the Directory Service log for matching entries.
Type: Error	Set to **y** to monitor for error events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for **Collect data**. The default is y.
Type: Warning	Set to **y** to monitor for warning events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for **Collect data**. The default is y.

Parameter	How To Set It
Type: Information	Set to **y** to monitor for information events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for **Collect data**. The default is n.
Type: Success Audit	Set to **y** to monitor for success audit events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for **Collect data**. The default is n.
Type: Failure Audit	Set to **y** to monitor for failure audit events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for **Collect data**. The default is n.
Instructions for filtering: To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log. The search string can contain criteria used to include entries, exclude entries, or both. • Separate include and exclude criteria with a colon (:). For example, `net:logon` • Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ` • If you are specifying only include criteria, the colon is not necessary. For example, `SQL` • If you are specifying only exclude criteria, start the search string with a colon. For example, `:defragmentation,cleanup`	
Event source filter	Specify one or more text strings to look for; separate multiple strings with commas. For example: `NTDS KCC,NTDS General`
Event category filter	Specify one or more text strings to look for; separate multiple strings with commas.
Event ID filter	Specify a single event ID or a range of event IDs; separate multiple entries by commas. For example: `1094,1404-1463`
Event user filter	Specify a single or multiple user names to look for; separate multiple entries by commas. For example: `Pat,Chris,Alex`
Computer filter	Specify a single or multiple computer names to look for; separate multiple entries by commas. For example: `SHASTA,MARS`
Event description filter	Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods; separate multiple entries with commas. For example: `data loss during system failures,corrupt indices,Inter-Site Transport objects failed`
Threshold - Maximum number of entries per event report	Specify the maximum number of Application log events that can be returned in each event report. The default is 30. For example, if this value is set to 30 and 67 Application log events are found, then three event reports are raised: two reports containing 30 events and one report containing seven events. The Message column on the **Events** tab in the Operator Console displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.
Event severity for log entries	Set the event severity level, from 1 to 40, to indicate the importance of the event. You may want to adjust the severity depending on which types of events you are checking for. The default is 8.

CUB_HealthCheck

Use this Knowledge Script to monitor the Unity Bridge service and the Digital Networking service. This script raises an event if either service is not running. In addition, this script generates data streams for service availability and can automatically restart a service that is down.

Resource Object

CISCOUNITYBRIDGE

Default Schedule

The default schedule is **Every minute**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Collect data?	Set to **y** to collect data about service status for charts and graphs. The default is y.
Auto-start the monitored services?	Set to **y** to auto-start any of the services that you choose to monitor. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which auto-start fails. The default is 5.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which auto-start succeeds. The default is 25.
Event severity when auto-start is set to "n"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager has not been set to restart the service. The default is 5.
Event severity when service doesn't exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service does not exist. The default is 25.
Monitor the Unity Bridge Service?	Set to **y** to monitor the Unity Bridge Service. The default is y.
Monitor the Digital Networking service?	Set to **y** to monitor the Digital Networking service. The default is y.

CUB_MemoryHigh

Use this Knowledge Script to monitor the memory that the Unity Bridge and Digital Networking processes are consuming. This script checks the memory used by each process individually, and the total memory used by both processes. If a process is not found, it assumes that the process is not running, and reports zero as the memory result.

Resource Object

CISCOUNITYBRIDGE

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Raise event if threshold exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.
Monitor Unity Bridge memory usage?	Set to **y** to monitor the memory usage of Unity Bridge. The default is y.
Threshold - Maximum memory usage for Unity Bridge	Specify the highest percentage of memory usage by Unity Bridge that can occur before an event is raised. The default is 200000 KB.
Threshold - Maximum memory pool usage for Unity Bridge	Specify the highest percentage of memory pool usage by Unity bridge that can occur before an event is raised. The default is 5000 KB.
Monitor Digital Networking memory usage?	Set to **y** to monitor the memory usage of Digital Networking. The default is y.
Threshold - Maximum memory usage for Digital Networking	Specify the highest percentage of memory usage by Digital Networking that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for Digital Networking	Specify the highest percentage of memory pool usage by Digital Networking that can occur before an event is raised. The default is 2500 KB.

CUB_RestartService

Use this Knowledge Script to schedule the Unity Bridge and Digital Networking services to stop and then restart after a specified interval. This script generates data streams for service availability.

Resource Object

CISCOUNITYBRIDGE

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Set to **y** to collect data for graphs and reports. The default is n.
Wait N seconds before restarting	Specify the number of seconds that should elapse before a service is restarted. The default is 5 seconds.
Event severity when stop fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager fails to stop a service. The default is 5.
Event severity when restart fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager fails to restart a service. The default is 5.
Event severity when status of service is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which service status is unavailable. The default is 10.
Event severity when stop succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops a service. The default is 25.
Event severity when restart succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts a service. The default is 25.
Restart …. service?	Set to **y** to restart the following services. The default is y. • **Unity Bridge** • **Digital Networking**

CUB_SystemUsage

Use this Knowledge Script to monitor CPU usage and memory for the Unity Bridge process, and for total CPU and memory usage. This script raises an event if a threshold is exceeded. In addition, this script generates a data stream for CPU and memory usage.

Resource Object

CISCOUNITYBRIDGE

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Raise event when threshold is exceeded?	Set to **y** to raise event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is y.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Threshold - Maximum Unity Bridge CPU usage	Specify the maximum Unity Bridge CPU usage that must occur before an event is raised. The default is 65%.
Threshold - Maximum total CPU usage	Specify the maximum total CPU usage that must occur before an event is raised. The default is 80%.
Threshold - Maximum Unity Bridge memory usage	Specify the maximum Unity Bridge memory usage that must occur before an event is raised. The default is 65%.
Threshold - Maximum total memory usage	Specify the maximum total memory usage that must occur before an event is raised. The default is 80%.

IIS_CpuHigh

Use this Knowledge Script to monitor CPU usage for IIS application processes. This script raises an event if a threshold is exceeded. In addition, this script generates a data stream for CPU usage for each process.

Resource Object

CISCOUNITYBRIDGE_IIST_Server

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Raise event if CPU usage exceeds threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If enabled, data collection returns CPU usage for the specified process. The default is n.
Process names	Enter the name of the application processes to monitor. Separate multiple entries with commas. For example: `inetinfo,dllhost`. The default is inetinfo. **Note** Do not append .exe to the process names.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU resources the selected process can use before an event is raised. The default is 60%.
Event severity when CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

IIS_HealthCheck

Use this Knowledge Script to check IIS servers, Web site status, and the queue length for blocked I/O requests. This script raises an event if any server or Web site is not running or if the blocked I/O queue length is longer than the specified threshold. In addition, this script can automatically restart the IIS server or Web site.

Note
This script monitors only Web sites (servers), not FTP sites, NNTP sites, or SMTP sites.

Resource Objects

- CISCOUNITYBRIDGE_IIST_Server
- CISCOUNITYBRIDGE_IIST_FTPSRV
- CISCOUNITYBRIDGE_IIST_W3SRV
- CISCOUNITYBRIDGE_IIST_WebInst

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Auto-start monitored server(s)?	Set to **y** to automatically restart down servers. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which auto-start fails. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which auto-start succeeds. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager has not been set to restart the service. The default is 18.
Event severity for blocked I/O requests	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Threshold - Maximum blocked I/O requests	Specify the maximum number of blocked I/O requests that can be in the queue before an event is raised. The default is 0 requests.
Monitor IIS server?	Set to **y** to monitor the IIS server. The default is y.
Monitor FTP server?	Set to **y** to monitor the FTP server. The default is n.

IIS_KillTopCPUProcs

Use this Knowledge Script to monitor the CPU usage for the IIS `dllhost` and `mtx` processes. This script raises an event if a threshold is exceeded and can automatically stop a process that exceeds the CPU usage threshold.

Resource Object

CISCOUNITYBRIDGE_IIST_Server

Default Schedule

The default schedule is **Every three minutes**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Raise event if kill is successful or unsuccessful?	Set to **y** to raise an event if the stop process is successful or unsuccessful. The default is y.
Kill CPU-intensive processes?	Set to **y** to automatically stop any process that exceeds the maximum CPU usage allowed. The default is n.
Threshold - Maximum CPU usage allowed	Specify the maximum percentage of CPU usage allowed by the `dllhost` and `mtx` processes before an event is raised. The default is 90%.
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 10.
Event severity when kill fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a process is exceeding the threshold and AppManager cannot stop the process. The default is 10.
Event severity when kill succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a process is exceeding the threshold and AppManager successfully stops the process. The default is 20.

IIS_MemoryHigh

Use this Knowledge Script to detect whether an IIS process has exceeded the memory usage threshold you set. This script monitors the number of bytes of memory being used by the specified process and raises an event if a threshold is exceeded. In addition, this script generates a data stream for memory usage for each specified process.

Resource Object

CISCOUNITYBRIDGE_IIST_Server

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Raise event if threshold exceeded?	Set to **y** to raise an event when a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, this script returns memory usage for each specified process. The default is n.
Process names	Enter the name of the application process to monitor. Use a comma to separate multiple entries — do not use spaces. For example: `inetinfo,dllhost`. The default is inetinfo. **Note** Do not append .exe to the process names.
Threshold - Maximum memory usage	Specify the maximum amount of memory the selected process can use before an event is raised. The default is 10000000 bytes.
Threshold - Maximum memory pool usage	Specify the maximum amount of memory pool the selected process can use before an event is raised. The default is 5000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.

IIS_RestartServer

Use this Knowledge Script to restart an IIS server. This script raises an event if the server either successfully restarts or fails to restart.

Resource Object

CISCOUNITYBRIDGE_IIST_Server

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Restart server?	Set to **y** to automatically restart a server that is down. The default is y.
Wait N seconds before restarting	Specify the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the stop attempt fails. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the restart attempt fails. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the service is unavailable. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the stop attempt succeeds. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the restart attempt succeeds. The default is 25.

IIS_ServiceUpTime

Use this Knowledge Script to monitor the uptime for Web sites and services. This script raises an event if uptime falls below the threshold. In addition, this script generates data stream for service uptime.

Note
This script runs on IIS versions 5 and later.

Resource Objects

- CISCOUNITYBRIDGE_IIST_WebInst
- CISCOUNITYBRIDGE_IIST_FTPInst

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Raise event if uptime falls below threshold?	Set to **y** to raise an event if uptime falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to **y**, the script returns how long a service has been running. The default is n.
Threshold - Minimum uptime	Specify the minimum amount number of seconds that discovered Web sites and services and FTP sites and services are required to be up to prevent an event from being raised. If uptime is less than this threshold, an event is raised. The default is 10000 seconds.
Event severity when uptime falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which uptime falls below the threshold. The default is 5.

Report_ServicesAvail

Use this Knowledge Script to display the average availability of Unity Bridge services within a time frame that you specify. This script displays the data collected by the CUB_HealthCheck script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Data Source	
Select data wizard	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select one or more Knowledge Scripts to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Decimal accuracy for % values	Enter the number of decimal places that you want to see in the values generated by this report. The default is 3.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CiscoUnityBridgeServicesAvailability.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set the report properties as desired. The default report name is Cisco Unity Bridge Services Availability.

Parameter	How To Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_SystemUsage

Use this Knowledge Script to display average CPU and memory usage within a time frame that you specify. This script displays the data collected by the CUB_SystemUsage script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once.**

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Data Source	
Select data wizard	Select the computers that you want to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select one or more Knowledge Scripts to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Charts	
Include % CPU chart?	Set to **y** to include a chart that details the CPU usage for the selected cluster. The default is y.
Include memory usage chart?	Set to **y** to include a chart that details the memory usage for the selected cluster. The default is y.
% CPU chart threshold	Specify the CPU percentage threshold to display on the charts in the report. The default is 0%.
Memory usage chart threshold	Specify the physical memory threshold in KB to display on the charts in the report. The default is 0 KB.
Chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Chart color scheme	Select a color scheme template. The default is NetIQ1.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of information in the report. The default is y.
Select output folder	Locate and select the output folder. The default folder name is CiscoUnityBridgeSystemUsage.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.

Parameter	How To Set It
Select properties	Set the report properties as desired. The default report name is Cisco Unity Bridge System Usage.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Chapter 27
CiscoUE Knowledge Scripts

AppManager for Cisco Unity Express provides the following Knowledge Scripts for monitoring Unity Express resources. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
BackupAndRestoreStatus	Monitors the status of Unity Express Backup and Restore operations.
DeviceUptime	Monitors the number of hours that a Unity Express device has been operational.
GDMStorageUsage	Monitors the storage usage of Unity Express general delivery mailboxes.
LicenseCompliance	Monitors the number or percentage of in-use voice mail licenses on a Unity Express device.
MessageActivity	Monitors the number of new, read, and deleted messages on a Unity Express device since the last reboot.
OrphanedMailboxes	Monitors for mailboxes on a Unity Express device that are not associated with an owner.
PortStatus	Monitors the registration status of all Unity Express ports for an associated Unified Communications Manager.
SubscriberStorageUsage	Monitors the storage usage of one or more Unity Express Subscriber mailboxes.
SystemUsage	Monitors the total CPU usage for a Unity Express device.
TotalStorageUsage	Monitors the total storage usage for a Unity Express device.
VoiceMailLogins	Monitors the number of failed and total voice mail login attempts for a Unity Express device.
VoiceMailSessionsInUse	Monitors concurrent voice mail sessions that are in use on a Unity Express device.
Recommended Knowledge Script Group	Performs essential monitoring of your Cisco Unity Express environment.

BackupAndRestoreStatus

Use this Knowledge Script to monitor the status of Unity Express Backup and Restore operations. If a new Backup or Restore operation is discovered, then this script raises an event that identifies the operation type, the operation's date/time stamp, and the results of the operation. In addition, this script generates a data stream for successful (1) or failed (0) Backup and Restore operations.

Resource Object

CiscoUE

Default Schedule

By default, this script runs every 24 hours.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BackupAndRestoreStatus job fails. The default is 5.
Monitor Backup/Restore Events	
Raise event if Backup/Restore succeeded?	Select **Yes** to raise an event if the Backup or Restore operation was successful. The default is Yes.
Event severity when Backup/ Restore succeeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Backup or Restore operation was successful. The default is 25.
Raise event if Backup/Restore failed?	Select **Yes** to raise an event if the Backup or Restore operation failed. The default is Yes.
Event severity when Backup/ Restore failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Backup or Restore operation failed. The default is 5.
Monitor Backup/Restore Status	
Data Collection	
Collect data for Backup/Restore history?	Select **Yes** to collect data about the history of the Backup or Restore operation for charts and reports. The default is unselected.

DeviceUptime

Use this Knowledge Script to monitor the number of hours that a Unity Express device has been operational. This script raises an event if the device reboots. In addition, this script generates a data stream for the number of hours a device has been operational.

Resource Object

CiscoUE

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DeviceUptime job fails. The default is 5.
Monitor Unity Express Reboot Events	
Raise event if device reboots?	Select **Yes** to raise an event if the device reboots. The default is Yes.
Event severity when device reboots	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Unity Express device reboots. The default is 25.
Monitor Unity Express Device Uptime	
Data Collection	
Collect data for uptime?	Select **Yes** to collect data about device uptime for charts and reports. The default is Yes.

GDMStorageUsage

Use this Knowledge Script to monitor the storage usage of one or more Unity Express general delivery mailboxes. This script raises an event if the storage usage exceeds the threshold. In addition, this script generates data streams for the storage usage percentage of all monitored mailboxes.

Resource Object

CiscoUE General Delivery Mailboxes

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the GDMStorageUsage job fails. The default is 5.
List of general delivery mailboxes to monitor	Provide a list of the owner names of the mailboxes that you want to monitor, separated by commas. If you want to monitor all mailboxes, leave this parameter blank.
Monitor General Delivery Mailbox Storage Usage	
Event Notification	
Raise event if storage usage exceeds threshold?	Select **Yes** to raise an event if the percentage of storage usage exceeds the threshold. The default is Yes.
Threshold - Maximum storage usage	Specify the maximum percentage of general delivery mailbox storage usage that can be detected before an event is raised. The default is 80%.
Event severity when storage usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of storage usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for storage usage?	Select **Yes** to collect data about storage usage for charts and reports. The default is Yes.

LicenseCompliance

Use this Knowledge Script to monitor the number or percentage of in-use voice mail licenses. This script raises an event if the number or percentage of in-use licenses exceeds the threshold. In addition, this script generates data streams for the total number of available licenses, the number of in-use licenses, and the percentage of in-use licenses.

Resource Object

CiscoUE

Default Schedule

By default, this script runs every 24 hours.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the LicenseCompliance job fails. The default is 5.
Monitor Total Voice Mail Licenses Available	
Data Collection	
Collect data for total voice mail licenses available?	Select **Yes** to collect data about available voice mail licenses for charts and reports. The default is unselected.
Monitor Number of Voice Mail Licenses in Use	
Event Notification	
Raise event if number of voice mail licenses in use exceeds threshold?	Select **Yes** to raise an event if the number of in-use voice mail licenses exceeds the threshold. The default is unselected
Threshold - Maximum number of voice mail licenses in use	Specify the maximum number of voice mail licenses that can be in use before an event is raised. The default is 25 licenses.
Event severity when number of voice mail licenses in use exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-use voice mail licenses exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of voice mail licenses in use	Select **Yes** to collect data about in-use voice mail licenses for charts and reports. The default is unselected.
Monitor Percent of Voice Mail Licenses in Use	
Event Notification	
Raise event if percent of voice mail licenses in use exceeds threshold?	Select **Yes** to raise an event if the percentage of in-use voice mail licenses exceeds the threshold. The default is Yes.

Parameter	How to Set It
Threshold - Maximum percent of voice mail licenses in use	Specify the maximum percentage of voice mail licenses that can be in use before an event is raised. The default is 80%.
Event severity when percent of voice mail licenses in use exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of in-use voice mail licenses exceeds the threshold. The default is 5.
Data Collection	
Collect data for percent of voice mail licenses in use	Select **Yes** to collect data about in-use voice mail licenses for charts and reports. The default is unselected.

MessageActivity

Use this Knowledge Script to monitor the number of new, read, and deleted messages on a Unity Express device since the last polling interval. This script raises an event if the number of messages exceeds the threshold. In addition, this script generates data streams for new, deleted, and read messages.

Resource Object

CiscoUE Mailbox Folder

Default Schedule

By default, this script runs every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MessageActivity job fails. The default is 5.
Monitor New Messages	
Event Notification	
Raise event if new messages exceed threshold?	Select **Yes** to raise an event if the number of new messages exceeds the threshold. The default is Yes.
Threshold - Maximum new messages	Specify the maximum number of new messages that can be detected before an event is raised. The default is 100 messages.
Event severity when new messages exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of new messages exceeds the threshold. The default is 15.
Data Collection	
Collect data for new messages?	Select **Yes** to collect data about new messages for charts and reports. The default is unselected.
Monitor Read Messages	
Event Notification	
Raise event if read messages exceed threshold?	Select **Yes** to raise an event if the number of read messages exceeds the threshold. The default is Yes.
Threshold - Maximum read messages	Specify the maximum number of read messages that can be detected before an event is raised. The default is 100 messages.
Event severity when read messages exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of read messages exceeds the threshold. The default is 15.
Data Collection	
Collect data for read messages?	Select **Yes** to collect data about read messages for charts and reports. The default is unselected.

Parameter	How to Set It
Monitor Deleted Messages	
Event Notification	
Raise event if deleted messages exceed threshold?	Select **Yes** to raise an event if the number of deleted messages exceeds the threshold. The default is Yes.
Threshold - Maximum deleted messages	Specify the maximum number of deleted messages that can be detected before an event is raised. The default is 100 messages.
Event severity when deleted messages exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of deleted messages exceeds the threshold. The default is 25.
Data Collection	
Collect data for deleted messages?	Select **Yes** to collect data about deleted messages for charts and reports. The default is unselected.

OrphanedMailboxes

Use this Knowledge Script to identify mailboxes that are not associated with an owner. This script raises an event if an orphaned mailbox is found. In addition, this script generates data streams for the number of orphaned mailboxes.

Resource Object

CiscoUE Mailbox Folder

Default Schedule

By default, this script runs every 24 hours.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the OrphanedMailboxes job fails. The default is 5.
Monitor Orphaned Mailboxes	
Event Notification	
Raise event if orphaned mailboxes are found?	Select **Yes** to raise an event if an orphaned mailbox is found. The default is Yes.
Event severity when orphaned mailboxes are found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an orphaned mailbox is found. The default is 15.
Data Collection	
Collect data for orphaned mailboxes?	Select **Yes** to collect data about orphaned mailboxes for charts and reports. The default is unselected.

PortStatus

Use this Knowledge Script to monitor the registration status of all Unity Express CTI ports for an associated Unified Communications Manager. This script raises an event if the status of any port changes. In addition, this script generates a data stream for the percentage of registered ports.

Resource Object

CiscoUE

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the PortStatus job fails. The default is 5.
Monitor Port Status Events	
Raise event if a port is not registered?	Select **Yes** to raise an event if a monitored port is not registered. The default is Yes.
Event severity when a port is not registered	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored port is not registered. The default is 5.
Raise event if an unregistered port becomes registered?	Select **Yes** to raise an event if the status of a monitored port changes from unregistered to registered. The default is Yes.
Event severity when an unregistered port becomes registered	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a monitored port changes from unregistered to registered. The default is 25.
Monitor Percentage of Ports Registered	
Data Collection	
Collect data for percentage of ports registered?	Select **Yes** to collect data about registered ports for charts and reports. The default is unselected.

SubscriberStorageUsage

Use this Knowledge Script to monitor the storage usage of one or more Unity Express subscriber mailboxes. This script raises an event if the percentage of mailbox storage usage exceeds the threshold. In addition, this script generates data streams for the percentage of individual mailbox storage usage for all monitored mailboxes.

Resource Object

CiscoUE Subscriber Mailboxes

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SubscriberStorageUsage job fails. The default is 5.
List of mailboxes to monitor	Enter a list of the owner names of the mailboxes that you want to monitor, separated by commas. To monitor all mailboxes, leave this parameter blank.
Monitor Subscriber Mailbox Storage Usage	
Event Notification	
Raise event if storage usage exceeds threshold?	Select **Yes** to raise an event if the percentage of Subscriber mailbox storage usage exceeds the threshold. The default is Yes.
Threshold - Maximum storage usage	Specify the maximum percentage of Subscriber mailbox storage usage that can be detected before an event is raised. The default is 80%.
Event severity when storage usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of Subscriber mailbox storage usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for storage usage?	Select **Yes** to collect data about Subscriber storage usage for charts and reports. The default is Yes.

SystemUsage

Use this Knowledge Script to monitor total CPU usage for a Unity Express device. This script raises an event if CPU usage exceeds the threshold. In addition, this script generates a data stream for the percentage of total CPU usage.

Resource Object

CiscoUE

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SystemUsage job fails. The default is 5.
Monitor Unity Express CPU Usage	
Event Notification	
Raise event if total CPU usage exceeds threshold?	Select **Yes** to raise an event if the total percentage of CPU usage exceeds the threshold. The default is Yes.
Event severity when total CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 10.
Threshold - Maximum total CPU usage	Specify the maximum percentage of CPU usage that can occur before an event is raised. The default is 80%.
Data Collection	
Collect data for total CPU usage?	Select **Yes** to collect data about CPU usage for charts and reports. The default is unselected.

TotalStorageUsage

Use this Knowledge Script to monitor the total storage usage for a Unity Express device. This script raises an event if the percentage of storage usage exceeds the threshold. In addition, this script generates data streams for the percentage of total storage usage.

Resource Object

CiscoUE Storage Capacity

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the TotalStorageUsage job fails. The default is 5.
Monitor Total Storage Usage	
Event Notification	
Raise event if storage usage exceeds threshold?	Select **Yes** to raise an event if the percentage of storage usage exceeds the threshold. The default is Yes.
Threshold - Maximum storage usage	Specify the maximum percentage of storage usage that can occur before an event is raised. The default is 80%.
Event severity when storage usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of storage usage exceeds the threshold. The default is 5.
Data Collection	
Collect data for storage usage?	Select **Yes** to collect data about storage usage for charts and reports. The default is Yes.

VoiceMailLogins

Use this Knowledge Script to monitor the number of failed and total voice mail login attempts for a Unity Express device. This script raises an event if the number of failed attempts exceeds the threshold. In addition, this script generates data streams for total Web and phone login attempts, and for password and username failures on Web and phone login attempts.

Resource Object

CiscoUE

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VoiceMailLogins job fails. The default is 5.
Monitor Total Voice Mail Web Login Attempts	
Event Notification	
Raise event if login attempts exceed threshold?	Select **Yes** to raise an event if the number of Web login attempts exceeds the threshold. The default is Yes.
Threshold - Maximum login attempts	Specify the maximum number of Web logins that can be attempted before an event is raised. The default is 50 attempts.
Event severity when login attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of Web login attempts exceeds the threshold. The default is 15.
Data Collection	
Collect data for total voice mail Web login attempts?	Select **Yes** to collect data about Web login attempts for charts and reports. The default is unselected.
Monitor Total Voice Mail Phone Login Attempts	
Event Notification	
Raise event if login attempts exceed threshold?	Select **Yes** to raise an event if the number of phone login attempts exceeds the threshold. The default is Yes.
Threshold - Maximum login attempts	Specify the maximum number of phone logins that can be attempted before an event is raised. The default is 50 attempts.
Event severity when login attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of phone login attempts exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for total voice mail phone login attempts?	Select **Yes** to collect data about phone login attempts for charts and reports. The default is unselected.
Monitor Password Failures on Voice Mail Web Login Attempts	
Event Notification	
Raise event if failed attempts exceed threshold?	Select **Yes** to raise an event if the number of password failures on Web login attempts exceeds the threshold. The default is Yes.
Threshold - Maximum failed attempts	Specify the maximum number of password failures on Web login attempts that can occur before an event is raised. The default is 3 failures.
Event severity when failed attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of password failures on Web login attempts exceeds the threshold. The default is 5.
Data Collection	
Collect data for password failures on voice mail Web login attempts?	Select **Yes** to collect data about password failures on Web login attempts for charts and reports. The default is unselected.
Monitor Username Failures on Voice Mail Web Login Attempts	
Event Notification	
Raise event if failed attempts exceed threshold?	Select **Yes** to raise an event if the number of username failures on Web login attempts exceeds the threshold. The default is Yes.
Threshold - Maximum failed attempts	Specify the maximum number of username failures on Web login attempts that can occur before an event is raised. The default is 3 failures.
Event severity when failed attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of username failures on Web login attempts exceeds the threshold. The default is 5.
Data Collection	
Collect data for username failures on voice mail Web login attempts?	Select **Yes** to collect data about username failures on Web login attempts for charts and reports. The default is unselected.
Monitor Password Failures on Voice Mail Phone Login Attempts	
Event Notification	
Raise event if failed attempts exceed threshold?	Select **Yes** to raise an event if the number of password failures on phone login attempts exceeds the threshold. The default is Yes.
Threshold - Maximum failed attempts	Specify the maximum number of password failures on phone login attempts that can occur before an event is raised. The default is 3 failures.
Event severity when failed attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of password failures on phone login attempts exceeds the threshold. The default is 5.
Data Collection	
Collect data for password failures on voice mail phone login attempts?	Select **Yes** to collect data about password failures on phone login attempts for charts and reports. The default is unselected.
Monitor Username Failures on Voice Mail Phone Login Attempts	
Event Notification	
Raise event if failed attempts exceed threshold?	Select **Yes** to raise an event if the number of username failures on phone login attempts exceeds the threshold. The default is Yes.
Threshold - Maximum failed attempts	Specify the maximum number of username failures on phone login attempts that can occur before an event is raised. The default is 3 failures.

Parameter	How to Set It
Event severity when failed attempts exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of username failures on phone login attempts exceeds the threshold. The default is 5.
Data Collection	
Collect data for username failures on voice mail phone login attempts?	Select **Yes** to collect data about username failures on phone login attempts for charts and reports. The default is unselected.

VoiceMailSessionsInUse

Use this Knowledge Script to monitor concurrent voice mail sessions that are in use on a Unity Express device. This script raises an event if the number or percentage of sessions exceeds the threshold. In addition, this script generates data streams for maximum allowed sessions and for the number and percentage of in-use sessions.

Resource Object

CiscoUE Voicemail Ports

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VoiceMailSessionsInUse job fails. The default is 5.
Monitor Maximum Allowed Voice Mail Sessions	
Data Collection	
Collect data for maximum allowed voice mail sessions?	Select **Yes** to collect data about allowed voice mail sessions for charts and reports. The default is Yes.
Monitor Number of Voice Mail Sessions in Use	
Event Notification	
Raise event if number of voice mail sessions in use exceeds threshold?	Select **Yes** to raise an event if the number of in-use voice mail sessions exceeds the threshold. The default is unselected.
Threshold - Maximum number of voice mail sessions in use	Specify the maximum number of voice mail sessions that can be in use before an event is raised. The default is 6 sessions.
Event severity when number of voice mail sessions in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of in-use voice mail sessions exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of voice mail sessions in use?	Select **Yes** to collect data about the number of in-use voice mail sessions for charts and reports. The default is Yes.
Monitor Percent of Voice Mail Sessions in Use	
Event Notification	
Raise event if percent of voice mail sessions in use exceeds threshold?	Select **Yes** to raise an event if the percentage of in-use voice mail sessions exceeds the threshold. The default is Yes.

Parameter	How to Set It
Threshold - Maximum percent of voice mail sessions in use	Specify the maximum percentage of voice mail sessions that can be in use before an event is raised. The default is 80%. **Note** For a four-port Unity Express device, assigning a threshold of 80% results in an event being raised when all four ports are in use. When three out of four ports are in use, the percentage drops to 75.
Event severity when percent of voice mail sessions in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of in-use voice mail sessions exceeds the threshold. The default is 5.
Data Collection	
Collect data for percent voice mail sessions in use?	Select **Yes** to collect data about the percentage of in-use voice mail sessions for charts and reports. The default is Yes.

Recommended Knowledge Script Group

The following Knowledge Scripts are members of the CiscoUE recommended Knowledge Script Group. You can find these scripts individually on the CiscoUE tab and in a group on the RECOMMENDED tab of the Operator Console.

- DeviceUptime
- PortStatus
- SystemUsage
- TotalStorageUsage
- VoiceMailLogins
- VoiceMailSessionsInUse

Note
Cisco Unified Communications Manager Express routers do not provide the data the PortStatus script monitors. If you are running the Recommended KSG on a Unified Communications Manager Express router, remove the PortStatus script from the group. For more information, see "PortStatus" on page 1404.

All scripts in the KSG have their parameters set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and run the KSG on a Cisco Unity Express resource.

The KSG enables a "best practices" usage of AppManager for monitoring your Cisco Unity Express environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the CiscoUE tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the CiscoUE tab are not affected.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the CiscoUE KSG and want to restore it to its original form, you can reinstall AppManager for Cisco Unity Express on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\CiscoUE` directory.

Chapter 28
CiscoPA Knowledge Scripts

The CiscoPA category provides the following Knowledge Scripts that retrieve information from Cisco Personal Assistant to help you better manage Personal Assistant. You can use the retrieved information to identify when services are down, when events have been logged, and when performance data exceeds thresholds.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
CPA_CallActivity	Monitors the total number of calls to Personal Assistant, as well as the number of calls to Personal Assistant that fail.
CPA_CallsTransferredToDTMF	Monitors the number of times Personal Assistant transferred a call to DTMF.
CPA_CpuHigh	Monitors the CPU resources that an application's processes are consuming.
CPA_DialByName	Monitors the total number of attempts to dial by name, as well as the number of attempts that fail.
CPA_EventLog	Monitors the event log entries from Personal Assistant during the past *n* hours.
CPA_FalseAcceptance	Monitors the number of times that a call was accepted incorrectly during.
CPA_HealthCheck	Monitors the status of Personal Assistant services. Can automatically restarts any down service.
CPA_LogInFailure	Monitors the total number of failed Personal Assistant login attempts.
CPA_MemoryHigh	Monitors the memory that an application's processes are consuming. If a process is not found, it assumes that the process is not running, and reports zero as the memory result.
CPA_NonSpeechSessions	Monitors the number of Personal Assistant non-speech sessions.
CPA_RestartService	Schedules a Personal Assistant service to stop and then restart after a specified interval.
CPA_Sessions	Monitors the total number of active sessions.
CPA_SpeechChannelCreateFailure	Monitors the number of times that Personal Assistant failed to create a speech channel.
CPA_SpeechRecognitionFailure	Monitors the number of times that the speech recognition software failed to understand a spoken command.
CPA_SystemUsage	Monitors CPU and memory usage for Personal Assistant services, as well as the entire system CPU and memory usage.

Knowledge Script	What It Does
CPA_TransferFailed	Monitors the number of times that Personal Assistant tried and failed to transfer a call.
CPA_VoiceMail	Monitors the total number of times voice mail was accessed, as well as the number of voice mail login failures.
IIS_CpuHigh	Monitors CPU usage for IIS applications.
IIS_HealthCheck	Monitors the blocked I/O requests queue and the status of IIS services and Web sites.
IIS_KillTopCPUProcs	Monitors CPU usage for IIS processes and stops processes that are using excessive CPU resources.
IIS_MemoryHigh	Monitors the memory usage and memory pool usage of a specified IIS application process. If a process is not found, this script assumes that the process is not running, and reports zero as the memory result.
IIS_RestartServer	Restarts an IIS server.
IIS_ServiceUpTime	Monitors Web sites and Web services uptime.
Report_CallActivity	Summarizes the "Calls Attempted" and "Calls Completed" data collected by the CPA_CallActivity script.
Report_ServicesAvailability	Summarizes the availability of Personal Assistant services within a time frame that you specify.
Report_SystemUsage	Summarizes CPU and memory usage for Personal Assistant services and the total system.

CPA_CallActivity

Use this Knowledge Script to monitor the total number of calls to Personal Assistant, as well as the number of calls to Personal Assistant that fail. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for call activity. To make the most of the data gathered by this script, run Report_CallActivity.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold exceeded?	Set to **y** to raise an event when the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is y.
Threshold - Maximum calls to Personal Assistant	Specify the maximum number of calls to Personal Assistant that can occur before an event is raised. The default is 50 calls.
Threshold - Maximum failed calls to Personal Assistant	Specify the maximum number of calls to Personal Assistant that can fail before an event is raised. The default is 10 calls.
Event severity when threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 25.

CPA_CallsTransferredToDTMF

Use this Knowledge Script to monitor the number of times that Personal Assistant transferred a call from speech recognition to DTMF (dual tone multi-frequency) response. This script raises an event if the number exceeds the specified threshold. In addition, this script generates a data stream for transferred calls.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data for transferred calls?	Set to **y** to collect about transferred calls data for reports and graphs. The default is n.
Threshold - Maximum calls transferred to DTMF	Specify the maximum number of calls that can be transferred to DTMF before an event is raised. The default is 100 calls.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of calls transferred to DTMF exceeds the threshold. The default is 15.

CPA_CpuHigh

Use this Knowledge Script to monitor CPU usage for the following applications:

- PAServer
- PASPRM
- PASPNLM
- PAWebAdmin
- PASPREC
- PASPCS
- recserver
- compilation-ser

This script raises an event if an application's CPU utilization exceeds the thresholds you set. This script monitors CPU usage for each process individually and the total CPU usage for all processes. If a process is not found, this script assumes that the process is not running, and reports zero as the CPU result.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data for CPU usage?	Set to **y** to collect data about CPU usage for reports and graphs. The default is n.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.
Threshold - Maximum CPU usage for PAServer	Specify the highest percentage of CPU usage for PAServer that can occur before an event is raised. Set to **0** if you do not want to monitor this process. The default is 80%.
Threshold - Maximum CPU usage for PASPRM	Specify the highest percentage of CPU usage for PASPRM that can occur before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.
Threshold - Maximum CPU usage for PASPNLM	Specify the highest amount of CPU usage for PASPNLM that can occur before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.
Threshold - Maximum CPU usage for PAWebAdmin	Specify the highest amount of CPU usage for PAWebAdmin that can occur before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.

Description	How To Set It
Threshold - Maximum CPU usage for PASPREC	Specify the highest amount of CPU usage for PASPREC that can occur before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.
Threshold - Maximum CPU usage for PASPCS	Specify the highest amount of CPU usage for PASPCS that can occur before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.
Threshold - Maximum CPU usage for recserver	Specify the highest amount of CPU usage for recserver that can occur before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.
Threshold - Maximum CPU usage for compilation-ser	Specify the highest amount of CPU usage for compilation-ser that can occur before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.

CPA_DialByName

Use this Knowledge Script to monitor the total number of attempts to dial by name, as well as the number of failed attempts to dial by name. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for total and failed attempts.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about dial-by-name attempts for reports and graphs. The default is n.
Threshold - Maximum attempts to dial by name	Specify the most attempts that can occur before an event is raised. The default is 50 attempts.
Threshold - Maximum failed attempts to dial by name	Specify the most failed attempts that can occur before an event is raised. The default is 10 attempts.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 25.

CPA_EventLog

Use this Knowledge Script to monitor event log entries from Personal Assistant during the past *n* hours. This script raises an event if log entries are detected. In addition, this script generates a data stream for log entries.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event for log entries?	Set to **y** to raise an event when the log contains entries for which you have filtered. The default is y.
Collect data?	Set to **y** to collect data about log entries for charts and graphs. The default is n.
Separate data?	Set to **y** to separate events entries from different log files into different data streams. If set to **n**, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. The default is n. For example, if you are monitoring both the System and Application logs, you may want to set this parameter to **y** so that events in the System log are tracked separately from events in the Application log.
Log source	Specify the event log you want to monitor. You can specify multiple event logs, separated by commas. For example: `System,Application`. The default is Application.
Type: Error	Set to **y** to monitor for error events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the **Collect data** parameter. The default is y.
Type: Warning	Set to **y** to monitor for warning events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the **Collect data** parameter. The default is y.
Type: Information	Set to **y** to monitor for information events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the **Collect data** parameter. The default is n.
Type: Success Audit	Set to **y** to monitor for success audit events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the **Collect data** parameter. The default is n.

Parameter	How To Set It
Type: Failure Audit	Set to **y** to monitor for failure audit events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the **Collect data** parameter. The default is n.
Instructions for filtering: To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log. The search string can contain criteria used to include entries, exclude entries, or both.· • Separate include and exclude criteria with a colon (:). For example, `net:logon`. • Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ`. • If you are specifying only include criteria, the colon is not necessary. For example, `SQL`. • If you are specifying only exclude criteria, start the search string with a colon. For example, `:defragmentation,cleanup`.	
Event source filter	Specify one or more text strings to look for; separate multiple strings with commas. For example: `NTDS KCC,NTDS General`
Event category filter	Specify one or more text strings to look for; separate multiple strings with commas.
Event ID filter	Specify a single event ID or a range of event IDs; separate multiple entries by commas. For example: `1094,1404-1463`
Event user filter	Specify a single or multiple user names to look for; separate multiple entries by commas. For example: `Pat,Chris,Alex`
Computer filter	Specify a single or multiple computer names to look for; separate multiple entries by commas. For example: `SHASTA,MARS`
Event description filter	Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods; separate multiple entries with commas. For example: `data loss during system failures,corrupt indices,Inter-Site Transport objects failed`
Maximum number of entries per event report	Specify the maximum number of Application log events that can be returned in each event report. For example, if this value is set to 30 and 67 Application log events are found, then three event reports are raised: two reports containing 30 events and one report containing seven events. The default is 30. The Message column on the **Events** tab in the Operator Console displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.
Event severity for log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the log contains entries for which you have filtered. You may want to adjust the severity depending on the types of events for which you are checking. The default is 8.

CPA_FalseAcceptance

Use this Knowledge Script to monitor the number of times during an interval that a call was accepted incorrectly. This script raises an event if the number of false acceptances exceeds the threshold. In addition, this script generates a data stream for false acceptances.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data for false acceptances?	Set to **y** to collect data about false acceptances for reports and graphs. The default is n.
Threshold - Maximum false acceptances	Specify the most false acceptances that can occur before an event is raised. The default is 10 acceptances.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of false acceptances exceeds the threshold. The default is 15.

CPA_HealthCheck

Use this Knowledge Script to monitor the status of the following Personal Assistant services:

- PAServer
- PASPRM
- PASPNLM
- PAWebAdmin
- PASPREC
- PASPCS
- American English, U.K. English, European French, Canadian French, and German localized services

You can choose to restart any service that is down. This script generates data streams for service availability. To make the most of that data, run Report_ServicesAvailability.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every one minute**.

Setting Parameter Values

Set the **Values** tab parameters as necessary.

Description	How To Set It
Collect data?	Set to **y** to collect data about service status for reports and graphs. The default is y.
Auto-start monitored service(s)?	Set to **y** to auto-start the services that you choose to monitor. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager has not been set to restart the service. The default is 5.
Event severity when service does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service for which you are monitoring does not exist. The default is 15.
Monitor Cisco PAServer service?	Set to **y** to monitor PAServer. The default is y.
Monitor Cisco PASPRM service?	Set to **y** to monitor PASPRM. The default is y.
Monitor Cisco PASPNLM service?	Set to **y** to monitor PASPNLM. The default is y.

Description	How To Set It
Monitor Cisco PAWebAdmin service?	Set to **y** to monitor PAWebAdmin. The default is y.
Monitor Cisco PASPREC service?	Set to **y** to monitor PASPREC. The default is y.
Monitor Cisco PASPCS service?	Set to **y** to monitor PASPCS. The default is y.
Monitor American English localized services?	Set to **y** to monitor American English services. The default is y.
Monitor U.K. English localized services?	Set to **y** to monitor U.K. English services. The default is n.
Monitor European French localized services?	Set to **y** to monitor European French services. The default is n.
Monitor Canadian French localized services?	Set to **y** to monitor Canadian French services. The default is n.
Monitor German localized services?	Set to **y** to monitor German services. The default is n.

CPA_LogInFailure

Use this Knowledge Script to monitor the total number of failed Personal Assistant login attempts. This script raises an event if the number of failed attempts exceeds the threshold. In addition, this script generates a data stream for failed attempts.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the **Values** tab parameters as necessary.

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data for failed attempts?	Set to **y** to collect data about failed attempts for reports and graphs. the default is n.
Threshold - Maximum failed login attempts	Specify the highest number of failed login attempts that can occur before an event is raised. The default is 10 attempts.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failed logins exceeds the threshold. The default is 15.

CPA_MemoryHigh

Use this Knowledge Script to monitor the memory usage of the following applications:

- PAServer
- PASPRM
- PASPNLM
- PAWebAdmin
- PASPREC
- PASPCS
- recserver
- compilation-ser

This script monitors the memory used by each process individually, and the total memory used by all processes. If a process is not found, this script assumes that the process is not running, and reports zero as the memory result.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about memory and memory pool usage for reports and graphs. The default is n.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. the default is 8.
Monitor Cisco PAServer memory usage?	Set to **y** to monitor the memory usage of the Cisco PAServer. The default is y.
Threshold - Maximum memory usage for PAServer	Specify the highest amount of memory usage for the Cisco PAServer that can occur before an event is raised. The default is 200000 KB.
Threshold - Maximum memory pool usage for PAServer	Specify the highest amount of memory pool usage for the PAServer that can occur before an event is raised. The default is 5000 KB.
Monitor Cisco PASPRM memory usage?	Set to **y** to monitor the memory usage of Cisco PASPRM. The default is y.
Threshold - Maximum memory usage for PASPRM	Specify the highest amount of memory usage for Cisco PASPRM that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for PASPRM	Specify the highest amount of memory pool usage for PASPRM that can occur before an event is raised. The default is 2500 KB.

Description	How To Set It
Monitor Cisco PASPNLM memory usage?	Set to **y** to monitor the memory usage for Cisco PASPNLM. The default is y.
Threshold - Maximum memory usage for PASPNLM	Specify the highest amount of memory usage for Cisco PASPNLM that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for PASPNLM	Specify the highest amount of memory pool usage for PASPNLM that can occur before an event is raised. The default is 2500 KB.
Monitor Cisco PAWebAdmin memory usage?	Set to **y** to monitor the memory usage of Cisco PAWebAdmin. The default is y.
Threshold - Maximum memory usage for PAWebAdmin	Specify the highest amount of memory usage for Cisco PAWebAdmin that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for PAWebAdmin	Specify the highest amount of memory pool usage for PAWebAdmin that can occur before an event is raised. The default is 2500 KB.
Monitor Cisco PASPREC memory usage?	Set to **y** to monitor the memory usage of Cisco PASPREC. The default is y.
Threshold - Maximum memory usage for PASPREC	Specify the highest amount of memory usage for Cisco PASPREC that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for PASPREC	Specify the highest amount of memory pool usage for PASPREC that can occur before an event is raised. The default is 2500 KB.
Monitor Cisco PASPCS memory usage?	Set to **y** to monitor the memory usage of Cisco PASPCS. The default is y.
Threshold - Maximum memory usage for PASPCS	Specify the highest amount of memory usage for Cisco PASPCS that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for PASPCS	Specify the highest amount of memory pool usage for PASPCS that can occur before an event is raised. The default is 2500 KB.
Monitor Cisco recserver memory usage?	Set to **y** to monitor the memory usage of Cisco recserver. The default is y.
Threshold - Maximum memory usage for recserver	Specify the highest amount of memory usage for Cisco recserver that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for recserver	Specify the highest amount of memory pool usage for recserver that can occur before an event is raised. The default is 2500 KB.
Monitor Cisco compilation-ser memory usage?	Set to **y** to monitor the memory usage of Cisco compilation-ser. The default is y.
Threshold - Maximum memory usage for compilation-ser	Specify the highest amount of memory usage for Cisco compilation-ser that can occur before an event is raised. The default is 100000 KB.
Threshold - Maximum memory pool usage for compilation-ser	Specify the highest amount of memory pool usage for compilation-ser that can occur before an event is raised. The default is 2500 KB.

CPA_NonSpeechSessions

Use this Knowledge Script to monitor the number of Personal Assistant non-speech sessions. This script raises an event if the number exceeds the specified threshold. In addition, this script generates a data stream for established sessions.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data for non-speech sessions?	Set to **y** to collect data about non-speech sessions for reports and graphs. The default is n.
Threshold - Maximum non-speech sessions	Specify the maximum number of non-speech sessions that can occur before an event is raised. The default is 100 sessions.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of non-speech sessions exceeds the threshold. The default is 15.

CPA_RestartService

Use this Knowledge Script to schedule one of the following Personal Assistant services to stop and then restart after a specified interval:

- PAServer
- PASPRM
- PASPNLM
- PAWebAdmin
- PASPREC
- PASPCS
- American English, U.K. English, European French, Canadian French, and German localized services

This script generates data streams for service availability, stops, starts, and restarts.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Collect data?	Set to **y** to collect data for reports and graphs. The default is n.
Wait N seconds before restarting	Specify the number of seconds that should elapse before restarting a service. The default is 5 seconds.
Event severity when stop fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager was unable to stop a service. The default is 5.
Event severity when restart fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager was unable to restart a service. The default is 5.
Event severity when service status is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a service is unavailable. The default is 10.
Event severity when stop succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stopped a service. The default is 25.
Event severity when restart succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarted a service. The default s 25.
Restart Cisco PAServer service?	Set to **y** to restart Cisco PAServer. The default is y.
Restart Cisco PASPRM service?	Set to **y** to restart Cisco PASPRM. The default is n.

Description	How To Set It
Restart Cisco PASPNLM service?	Set to **y** to restart Cisco PASPNLM. The default is n.
Restart Cisco PAWebAdmin service?	Set to **y** to restart Cisco PAWebAdmin. The default is n.
Restart Cisco PASPREC service?	Set to **y** to restart Cisco PASPREC. The default is n.
Restart Cisco PASPCS service?	Set to **y** to restart Cisco PASPCS. The default is n.
Restart American English localized services?	Set to **y** to restart American English services. The default is y.
Restart U.K. English localized services?	Set to **y** to restart U.K. English services. The default is n.
Restart European French localized services?	Set to **y** to restart European French services. The default is n.
Restart Canadian French localized services?	Set to **y** to restart Canadian French services. The default is n.
Restart German localized services?	Set to **y** to restart German services. The default is n.

CPA_Sessions

Use this Knowledge Script to monitor the total number of active Personal Assistant sessions. This script raises an event if the number of sessions exceeds the threshold. In addition, this script generates a data stream for active sessions.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data for active sessions?	Set to **y** to collect data about active sessions for reports and graphs. The default is n.
Threshold - Maximum active sessions	Specify the maximum number of sessions that can be active before an event is raised. The default is 10 sessions.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active sessions exceeds the threshold. The default is 25.

CPA_SpeechChannelCreateFailure

Use this Knowledge Script to monitor the number of times that Personal Assistant failed to create a speech channel. This script raises an event if the number of failures exceeds the threshold. In addition, this script generates a data stream for failures.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data for speech channel creation failures?	Set to **y** to collect data about speech channel creation failures for reports and graphs. The default is n.
Threshold - Maximum speech channel creation failures	Specify the most failures that can occur before an event is raised. The default is 10 failures.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failures exceeds the threshold. The default is 15.

CPA_SpeechRecognitionFailure

Use this Knowledge Script to monitor the number of times that the speech recognition software failed to understand a spoken command. This script raises an event if the number of failures exceeds the threshold. In addition, this script generates a data stream for failures.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data for speech recognition failures?	Set to **y to** collect data about speech recognition failures for reports and graphs. The default is n.
Threshold - Maximum speech recognition failures	Specify the most failures that can occur before an event is raised. The default is 10 failures.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failures exceeds the threshold. The default is 15.

CPA_SystemUsage

Use this Knowledge Script to monitor CPU and memory usage for Personal Assistant services, as well as the total system CPU and memory usage. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for CPU and memory usage. To make the most of this data, run Report_SystemUsage.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, this script returns CPU and/or memory usage for the specified process. The default is y.
Event severity when threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 10.
Threshold - Maximum Personal Assistant CPU usage	Specify the highest percentage of Personal Assistant CPU usage that can occur before an event is raised. The default is 65%.
Threshold - Maximum total CPU usage	Specify the highest percentage of total CPU usage that can occur before an event is raised. The default is 80%.
Threshold - Maximum Personal Assistant memory usage	Specify the highest percentage of Personal Assistant memory usage that can occur before an event is raised. The default is 65%.
Threshold - Maximum total memory usage	Specify the highest percentage of total memory usage that can occur before an event is raised. The default is 80%.

CPA_TransferFailed

Use this Knowledge Script to monitor the number of times that Personal Assistant tried and failed to transfer a call during an interval. This script raises an event if the number of failures exceeds the threshold. In addition, this script generates a data stream for transfer failures.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise events. The default is y.
Collect data for transfer failures?	Set to **y** to collect data about transfer failures for reports and graphs. The default is n.
Threshold - Maximum failed call transfer attempts	Specify the most attempts that can fail before an event is raised. The default is 10 attempts.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failed attempts exceeds the threshold. The default is 15.

CPA_VoiceMail

Use this Knowledge Script to monitor the total number of voice mail accesses, as well as the number of voice mail login failures. This script raises an event if either threshold is exceeded. In addition, this script generates data streams for voice mail accesses and failures.

Resource Object

CiscoPersonalAsst

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event when a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about voice mail accesses and login failures for reports and graphs. The default is n.
Threshold - Maximum voice mail access attempts	Specify the most attempts that can occur before an event is raised. The default is 50 attempts.
Threshold - Maximum failed voice mail logins	Specify the most login failures that can occur before an event is raised. The default is 10 failures.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.

IIS_CpuHigh

Use this Knowledge Script to monitor CPU usage for IIS application processes. This script raises an event if CPU usage exceeds the threshold. In addition, this script generates a data stream for CPU usage.

Resource Object

CPA_IIST_Server

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if CPU usage exceeds threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data for CPU usage?	Set to **y** to collect data about CPU usage for reports and graphs. The default is n.
Process names	Specify the name of the application processes you want to monitor. Separate multiple entries with commas. For example: `inetinfo,dllhost`. The default is inetinfo. **Note** Do not append `.exe` to the process names.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU resources the selected process can use before an event is raised. The default is 60%.
Event severity when CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 8.

IIS_HealthCheck

Use this Knowledge Script to check IIS servers, Web site status, and the queue length for blocked I/O requests. This script raises an event if any server or Web site is not running and if the blocked I/O queue length is longer than the specified threshold. In addition, this script can automatically restart the IIS server or Web site.

This script monitors only Web sites (servers), not FTP sites, NNTP sites, or SMTP sites.

Resource Objects

- CPA_IIST_Server
- CPA_IIST_FTPSRV
- CPA_IIST_W3SRV
- CPA_IIST_WebInst

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Auto-start monitored server(s)?	Set to **y** to automatically restart servers that are down. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager has not been set to restart the service. The default is 18.
Event severity for blocked I/O requests	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of blocked I/O requests exceeds the threshold. The default is 5.
Threshold - Maximum blocked I/O requests	Specify the maximum number of blocked I/O requests that can be in queue before an event is raised. The default is 0 requests.
Monitor IIS server?	Set to **y** to monitor the IIS server. The default is y.
Monitor FTP server?	Set to **y** to monitor the FTP server. The default is n.

IIS_KillTopCPUProcs

Use this Knowledge Script to monitor the CPU usage for the IIS `dllhost` and `mtx` processes. This script raises an event if a threshold is exceeded. In addition, this script can automatically stop a process that exceeds the CPU usage threshold.

Resource Object

CPA_IIST_Server

Default Schedule

The default schedule is **Every three minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if kill is successful or unsuccessful?	Set to **y** to raise an event if a service is successfully or unsuccessfully stopped. The default is y.
Kill CPU-intensive processes?	Set to **y** to automatically stop any process that exceeds the threshold. The default is n.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU usage by the `dllhost` and `mtx` processes that can be detected before an event is raised. The default is 90%.
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CPU usage exceeds the threshold. The default is 10.
Event severity when kill fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the process. The default is 10.
Event severity when kill succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the process. The default is 20.

IIS_MemoryHigh

Use this Knowledge Script to monitor the memory usage of IIS processes. This script raises an event if a threshold is exceeded. In addition, this script generates a data stream for memory usage.

Resource Object

CPA_IIST_Server

Default Schedule

The default schedule is **Every three minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about memory usage for reports and graphs. The default is n.
Process names	Specify the name of the application process to monitor. Use a comma to separate multiple entries — do not use spaces. For example: `inetinfo,dllhost`. The default is inetinfo. **Note** Do not append `.exe` to the process names.
Threshold - Maximum memory usage	Specify the maximum amount of memory usage a process can use before an event is raised. The default is 10000000 bytes.
Threshold - Maximum memory pool usage	Specify the maximum amount of memory pool a process can use before an event is raised. The default is 5000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.

IIS_RestartServer

Use this Knowledge Script to restart an IIS server. This script raises an event if the server successfully restarts or fails to restart.

Resource Object

CPA_IIST_Server

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Wait N seconds before restarting	Specify the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the server. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart the server. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the server. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the server. The default is 25.
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the server. The default is 25.

IIS_ServiceUpTime

Use this Knowledge Script to monitor the uptime for Web sites and services. This script raises an event if uptime falls below the threshold that you set. In addition, this script generates a data stream for uptime.

Resource Objects

- CPA_IIST_WebInst
- CPA_IIST_FTPInst

Note
This script runs on IIS version 5 and later.

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Raise event if uptime falls below threshold?	Set to **y** to raise an event if uptime falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, the script returns how long a service has been running. The default is n.
Threshold - Minimum uptime	Specify the minimum amount of time that discovered Web sites and services and FTP sites and services must be up to prevent an event from being raised. If the sites and services uptime is less than this threshold, an event is raised. The default is 10000 seconds.
Event severity when uptime falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which uptime falls below the threshold. The default is 5.

Report_CallActivity

Use this Knowledge Script to summarize number of attempted and failed calls to Personal Assistant within a time frame that you specify. This script uses the data gathered by the CPA_CallActivity script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select data wizard	Select the data for your report, either by view, computer, or data group. The default is View.
Select Knowledge Script	Select the scripts that you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is CPACallActivity.
Select properties	Set the properties parameters as desired. The default report name is Cisco Personal Assistant Call Activity.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report is successful?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is created successfully. The default is 35.

Description	How To Set It
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report was not created. The default is 5.

Report_ServicesAvailability

Use this Knowledge Script to summarize the availability of Personal Assistant services within a time frame that you specify. This script uses the data gathered by the CPA_HealthCheck script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select data wizard	Select the data for your report, either by view, computer, or data group. The default is View.
Knowledge Script(s)	Select the scripts that you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding
Report Settings	
Decimal accuracy for % values	Specify the number of decimal places that you want to see in the values generated by this report. The default is 3.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set options for the output folder. The default folder name is CiscoPAServicesAvailability.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set the report properties as desired. The default report name is Cisco Personal Assistant Services Availability.

Description	How To Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report is successful?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is created successfully. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report was not created. The default is 5.

Report_SystemUsage

Use this Knowledge Script to summarize CPU and memory usage for Personal Assistant services and the total system. This script uses the data gathered by the CPA_SystemUsage script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select data wizard	Select the data for your report, either by view, computer, or data group. The default is View.
Knowledge Script(s)	Select the scripts that you want to use for the report. Select only those scripts that are applicable to this Report script.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding
Report Settings	
Include % CPU chart?	Select whether to display a CPU usage chart in the report. The default is y.
Include memory usage chart?	Select whether to display a memory usage chart in the report. The default is y.
% CPU chart threshold	Specify the CPU percentage threshold to display on the charts in the report. The default is 0%.
Memory usage chart threshold	Specify the memory threshold in KB to display on the charts in the report. The default is 0 KB.
Chart size	Select the size of the rendered chart. Choose from **Large**, **Medium**, and **Small**. The default is Medium.
Chart color scheme	Select a color scheme template. The default template is NetIQ1.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the Report script. The default is y.
Include table?	Set to **y** to include a table of information in the report. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default folder name is `CiscoPersonalAssistantSystemUsage`.
Select properties	Set the report properties as desired. The default report name is Cisco Personal Assistant System Usage.

Description	How To Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report is successful?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is created successfully. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report was not created. The default is 5.

Chapter 29
Citrix MetaFrame Knowledge Scripts

AppManager for Citrix MetaFrame (MFXP) provides the following Knowledge Scripts for monitoring servers that are running Citrix MetaFrame or Presentation Server.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ApplicationUsersHigh	Monitors the number of users running an application across all sessions.
BytesTransferredPerUser	Monitors the number of bytes per user transferred between client computers and XenApp or Presentation Server.
DataCollectorChanged	Monitors whether a zone's data collector has changed since the last monitoring interval.
DefaultDataCollector	Identifies the default data collector for a XenApp or Presentation Server.
FarmUserLoad	Monitors the number of users connected to each XenApp or Presentation Server in a server farm.
ICAAvgLatencyHigh	Monitors the average latency of ICA sessions on XenApp or Presentation Server.
ICALatencyHigh	Monitors the most-recent measure of latency for ICA sessions on XenApp or Presentation Server.
LicenseInUseHigh	Monitors the percentage of licenses in use for Presentation Server 4.0 and later.
PublishedApplicationDetails	Searches for specified applications that are on the list of published applications for Citrix Server farms.
ServerFarmHealth	Monitors the health and availability of Citrix Server services in a designated server farm and monitors the farm for servers that are not responding.
ServerProcessesHigh	Monitors the number of processes on XenApp or Presentation Server across all sessions.
ServerProcessesResourceHigh	Monitors the use of CPU and memory resources by processes on XenApp or Presentation Server.
ServerSessionsHigh	Monitors the number of sessions on XenApp or Presentation Server.
SessionPerUser	Monitors the number of sessions on XenApp or Presentation Server that are open for each user.

Knowledge Script	What It Does
SessionState	Monitors the number of sessions matching specified states.
UserResourcesHigh	Monitors the use of CPU and memory resources by users connected to Citrix Presentation Server or XenApp server.

ApplicationUsersHigh

Use this Knowledge Script to monitor the number of users across all sessions running applications published on Citrix Presentation Server or XenApp server. If the number of users falls below the minimum threshold or exceeds the maximum threshold, an event is raised.

Note
To gather data about all sessions on a specific Citrix server in a Citrix farm, run this Knowledge Script on that individual server in the farm.

If you are monitoring multiple applications, separate events are raised for each application. The same thresholds apply to all applications.

Resource Objects

Citrix Presentation Server Applications object or individual applications

Citrix XenApp Applications object or individual applications

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if number of users exceeds or falls below threshold?	Select **Yes** to raise an event when the number of users running an application falls below the minimum threshold or exceeds the maximum threshold you set. The default is Yes.
Event severity when number of users exceeds or falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).
Data Collection	
Collect data for number of users?	Select **Yes** to collect data for charts and reports. If enabled, returns information about the number of users running an application. The default is Yes.
Monitoring	
Threshold -- Minimum number of users	Specify the minimum number of users across all sessions that can be running a published application before an event is raised. The value can range from 0 to 99999 users. The default is 5.
Threshold -- Maximum number of users	Specify the maximum number of users across all sessions that can be running a published application before an event is raised. The default is 50.

BytesTransferredPerUser

Use this Knowledge Script to monitor the number of bytes per user transferred between client computers and the Citrix MetaFrame server or Citrix Presentation Server.

The number of bytes is calculated by taking the total of all bytes for all Independent Computing Architecture (ICA) sessions currently active for a user. For each user with one or more ICA protocol sessions on XenApp or Presentation Server, the sum of bytes transferred by all sessions associated with that user is compared to the threshold you set. If the number of bytes exceeds the threshold, an event is raised.

Resource Objects

Citrix Presentation Server object

Citrix XenApp object

Default Schedule

The default schedule is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if the total number of bytes transferred for a user exceeds threshold?	Select **Yes** to raise an event if the total bytes per user exceeds the threshold. The default is Yes.
Event severity when the total number of bytes transferred for a user exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the total bytes per user exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for bytes transferred per user?	Select **Yes** to collect data for charts and reports. If enabled, returns information about the number of bytes per user transferred between ICA clients and XenApp or Presentation Server. The default is unselected.
Monitoring	
Threshold -- Maximum bytes transferred per user	Specify the maximum number of bytes that can be transferred per user before an event is raised. The default is 10485760 bytes.

DataCollectorChanged

Use this Knowledge Script to determine whether the data collector for a Citrix XenApp server or Presentation Server zone has changed since the last time the script was run. If a change to the data collector for the selected zone is detected, an event is raised.

Resource Objects

Citrix Presentation Server Zones object or individual zones

Citrix XenApp Zones object or individual zones

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if a change to the data collector is detected?	Select **Yes** to raise an event if a change to the data collector for this server zone has occurred since the last monitoring interval. The default is Yes.
Event severity when a change is detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a change to the data collector occurs. The default is 5.
Data Collection	
Collect data for data collector changes?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns one of the following values: • **100** if the data collector has changed • **0** if the data collector has not changed The default is unselected.

DefaultDataCollector

Use this Knowledge Script to identify the default data collector for a specific Citrix XenApp server or Presentation Server under a Citrix farm, or to identify *all* available XenApp servers or Presentation Servers under a Citrix farm. The default data collector was called the *master browser* in versions prior to Citrix Presentation Server 4.0.

This script raises an event if the default data collector information is found, and the event message includes default data collector and zone information for the selected XenApp server or Presentation Server.

If you run this script on the Server Object, the event returns the zone name and the default data collector for all the servers that are discovered under Server Object. If you run this script on a particular server or set of servers, the event returns the zone name and default data collector for those servers only.

Resource Object

Citrix Presentation Server Servers object or individual servers

Citrix XenApp Servers object or individual servers

Default Schedule

By default, this script is only run once for each server.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Event severity when default data collector information is found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the default data collector information is found. The default is 15.
Event severity when user is not a Citrix farm administrator	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the user is not a Citrix farm administrator. The default is 11.
Event severity when the job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event if the job fails unexpectedly. The default is 5.

FarmUserLoad

Use this Knowledge Script to monitor the number of users connected to each Citrix XenApp or Presentation Server in a server farm. You can set thresholds for the minimum and maximum number of users. An event is raised if the maximum threshold is exceeded or the minimum threshold is not met.

In addition, you can set thresholds based on a standard deviation, calculated from the number of users connected to each server in the farm since the first job iteration. The maximum and minimum thresholds for individual servers are defined by the number of standard deviations above or below the average number of users connected to all servers since the first iteration of the job.

If you use the standard deviation thresholds, the thresholds for the minimum and maximum numbers of users are ignored.

You can also specify servers in a farm that are to be excluded from monitoring by this Knowledge Script.

Resource Object

Citrix Presentation Server Farm object

Citrix XenApp Farm object

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if any threshold exceeded or not met?	Select **Yes** to raise an event if the number of standard deviations or the number of users exceeds or falls below one of the thresholds you set. The default is Yes.
Event severity when one of the thresholds is exceeded or is not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of standard deviations or the number of users exceeds or falls below a threshold. The default is 5.
Data Collection	
Collect data for number of users?	Select **Yes** to collect data for charts and reports. If enabled, returns the numbers of users connected to XenApp or Presentation Servers. The default is unselected.
Monitoring	
Type of threshold to use?	Select the type of threshold to use: • Standard Deviation • Minimum/Maximum The default is `Minimum/Maximum`.
Standard Deviation Settings	

Description	How to Set It
Threshold -- Number of standard deviations below average	Specify the number of standard deviations below the average number of users connected to all servers in the farm. If the number of users of a particular server falls below this threshold, an event is raised. The default is 1.
Threshold -- Number of standard deviations above average	Specify the number of standard deviations above the average number of users connected to all servers in the farm. If the number of users of a particular server exceeds this threshold, an event is raised. The default is 1.
Minimum/Maximum Settings	
Threshold -- Minimum number of users	Specify the minimum number of users who must be connected to a server before an event is raised. The default is 10 users.
Threshold -- Maximum number of users	Specify the maximum number of users who can be connected to a server before an event is raised. The default is 50 users.
Servers to exclude (comma-separated, no spaces)	Provide a list of server names, separated by commas and no spaces (for example, `MFServer1,MFServer2,MFServer3`). Servers specified in this parameter are not monitored by this Knowledge Script.

ICAAvgLatencyHigh

Use this Knowledge Script to monitor the average latency, in milliseconds, for Independent Computing Architecture (ICA) sessions on a Citrix Presentation Server or XenApp server. Latency refers to the delay between user input such as, mouse movement or keyboard strokes, and screen refresh.

Each time this Knowledge Script runs, it checks the average latency of each ICA session for the length of time the session has been open. If the average latency of any session exceeds the threshold you set, an event is raised.

Use the ICALatencyHigh Knowledge Script to monitor the most recently measured latency for each ICA session. If latency consistently exceeds the threshold you set, you can use the Citrix SpeedScreen Latency Reduction Manager to adjust your SpeedScreen settings.

Resource Objects

Citrix Presentation Server object

Citrix XenApp object

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if average latency exceeds threshold?	Select **Yes** to raise an event if the average latency for ICA sessions exceeds the threshold. The default is Yes.
Event severity when average latency exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average latency exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for average latency?	Select **Yes** to collect data for charts and reports. If enabled, returns the average latency of each ICA session for the length of time the session has been open. The default is unselected.
Monitoring	
Threshold -- Maximum average latency of ICA sessions	Specify a maximum threshold, in milliseconds, for the average latency for any ICA session. The default is 30 milliseconds.

ICALatencyHigh

Use this Knowledge Script to monitor the most recent or current measure of latency for each Independent Computing Architecture (ICA) session on a Citrix MetaFrame server or Presentation Server. Latency refers to the delay between user input, such as mouse movement or keyboard strokes, and screen refresh.

If the most recent measure of latency for any ICA session exceeds the threshold you set, an event is raised.

Use the ICAAvgLatencyHigh Knowledge Script to monitor the average latency of all ICA sessions over time. If latency consistently exceeds the threshold you set, you can use the SpeedScreen Latency Reduction Manager to adjust your SpeedScreen settings.

Resource Objects

Citrix Presentation Server object

Citrix XenApp object

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if current latency exceeds threshold?	Select **Yes** to raise an event if the current latency for any ICA session exceeds the threshold. The default is Yes.
Event severity when current latency exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which latency exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for current latency of ICA sessions?	Select **Yes** to collect data for charts and reports. If enabled, returns the most recent measure of latency for each ICA session. The default is unselected.
Monitoring	
Threshold -- Maximum current latency of an ICA session	Specify the maximum latency amount (in milliseconds) any ICA session can have before an event is raised. The default is 30.

LicenseInUseHigh

Use this Knowledge Script to monitor the percentage of licenses in use for Citrix XenApp and Presentation Server. If the percentage of licenses in use exceeds the threshold you set, an event is raised.

Citrix XenApp and Presentation Server use a license server with license files that grant connection rights to a client. When a client connects to the server, one license is allocated. License servers can be shared by multiple server farms, and in such a case, a client can connect to either farm and consume only one license.

LicenseInUseHigh is cluster-aware. It monitors and collects data for active nodes, for all the available license types on the server. Even if you have two child jobs for LicenseInUseHigh, the script monitors and collects data for active nodes only. The LicenseInUseHigh job does not stop if the state of the cluster node changes, such as when the passive node of the cluster becomes active, or the active node becomes passive. In the event of a failover, LicenseInUseHigh monitors all the license types available on the server.

If data collection is enabled, this Knowledge Script returns the percentage of licenses in use compared to the total number of licenses available on the license server.

This Knowledge Script only monitors Citrix XenApp 5.0 and Citrix Presentation Server 4.5.

Resource Object

For clustered environments:

- Citrix Presentation server License object
- Citrix XenApp License object

For non-clustered environments:

- Citrix Presentation Server License object or individual license files
- Citrix XenApp License object or individual license files

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if percentage of licenses in use exceeds threshold?	Select **Yes** to raise an event if the percentage of licenses in use exceeds the threshold. The default is Yes.
Event severity when percentage of licenses in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of licenses in use exceeds the threshold. The default is 5.
Data Collection	
Collect data for percentage of licenses in use?	Select **Yes** to collect data for charts and reports. If enabled, returns the percentage of licenses in use. The default is unselected.

Description	How to Set It
Monitoring	
Threshold -- Maximum percentage of licenses in use	Specify the maximum percentage of licenses that can be in use before an event is raised. The default is 80%.

PublishedApplicationDetails

This Knowledge Script searches for specified applications that are on the list of published applications for Citrix Server farms. This script raises an event that lists details about the published application or the list of applications, including the name of the farms and servers on which the application has been published.

Resource Objects

Citrix Presentation Server Farm object

Citrix XenApp Farm object

Default Schedule

By default, this script is only run once for each server.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Applications to be verified in the published application list (comma-separated)	Type the name of the application or applications for which you want to determine is in the published application list. For more than one application, separate the application names with a comma, no space. This parameter supports the wild card characters "*" and "?" for published applications.
Event Notification	
Event severity when specified application details are found	Set the event severity level, from 1 to 40, to indicate the importance of the event raised when specific application details are found. The default is 15.
Event severity when user is not a Citrix farm administrator	Set the event severity level, from 1 to 40, to indicate the importance of the event raised when the user is not a Citrix Farm Administrator. The default is 11.
Event severity when the job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of the event in which this job fails unexpectedly. The default is 5.

ServerFarmHealth

Use this Knowledge Script to monitor a Citrix Presentation Server or XenApp server farm for unresponsive servers. You can set two thresholds for non-responding servers:

- The maximum number of servers that are unresponsive before a **warning** event is raised
- The maximum number of servers that are unresponsive before an **error** event is raised

This script raises an event if either threshold is exceeded. You can set severity levels for each event type.

You can also use this script to monitor the health and availability of the following services in a designated farm. The services in a designated farm must be running before you can collect data.

- Client Network
- Encryption
- Independent Management Architecture
- MFCOM (XenApp Management SDK)
- Licensing

Each service can display one of the following statuses:

- **Running —** The service is running.
- **Not running —** The service is not running.
- **SCM_Fail —** The service cannot establish a connection to the Service Control Manager (SCM), which monitors all Citrix Server services.
- **SRV_Fail —** The service establishes a connection to the Service Control Manager (SCM), but fails to establish a connection to the service.

Resource Objects

Citrix Presentation Server Farm object

Citrix XenApp Farm object

Default Schedule

The default schedule is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if number of servers not responding exceeds threshold?	Select **Yes** to raise an event if the number of unresponsive servers exceeds the thresholds you set. The default is Yes.
Raise event to display the status of Citrix Server services in a farm?	Select **Yes** to raise an event to display the status of Citrix Server services in a designated farm. The default is Yes.

Description	How to Set It
Warning event severity when the threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the warning threshold is exceeded. The default is 11.
Error event severity when the threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the error threshold is exceeded. The default is 5.
Event severity when the service is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Citrix Server service is down. The default is 5.
Data Collection	
Collect data for servers not responding?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of servers in the server farm that are down. If any servers are down, the data details include the names and IP addresses of servers that are unresponsive. The default is unselected.
Collect data for Citrix Server services in a farm?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of Citrix Server services in the farm that are down. The default is unselected.
Monitoring	
Servers to ignore	Provide a list of servers you do not want to monitor. Use commas with no spaces to separate server names in a list. For example, `MFServer1,MFServer2,MFServer3`. You can also click **Browse [...]** to use a network browser to select computer names.
Services to Ignore	
Ignore Client Network Service?	Select **Yes** to allow the script to ignore the Client Network Service during monitoring of the selected Citrix Server. The default is unselected. This option is useful when the Client Network Service is on a different server than the one you are monitoring. When this option is enabled, the ServerFarmHealth job does not raise an event if it cannot locate the Client Network Service.
Ignore Encryption Service?	Select **Yes** to allow the script to ignore the Encryption Service during monitoring of the selected Citrix Server. The default is unselected. This option is useful when the Encryption Service is on a different server than the one you are monitoring. When this option is enabled, the ServerFarmHealth job does not raise an event if it cannot locate the Encryption Service.
Ignore Independent Management Architecture Service?	Select **Yes** to allow the script to ignore the Independent Management Architecture Service during monitoring of the selected Citrix Server. The default is unselected. This option is useful when the Independent Management Architecture Service is on a different server than the one you are monitoring. When this option is enabled, the ServerFarmHealth job does not raise an event if it cannot locate the Independent Management Architecture Service.

Description	How to Set It
Ignore MFCom Service?	Select **Yes** to allow the script to ignore the MFCom Service during monitoring of the selected Citrix Server. The default is unselected. This option is useful when the MFCom Service is on a different server than the one you are monitoring. When this option is enabled, the ServerFarmHealth job does not raise an event if it cannot locate the MFCom Service.
Ignore Citrix Licensing Service?	Select **Yes** to allow the script to ignore the Citrix Licensing Service during monitoring of the selected Citrix Server. The default is unselected. This option is useful when the Citrix Licensing Service is on a different server than the one you are monitoring. When this option is enabled, the ServerFarmHealth job does not raise an event if it cannot locate the Citrix Licensing Service.
Warning event threshold -- Maximum number of servers not responding	Specify the maximum number of servers that can be detected down before a warning event is raised. The default is 3 servers.
Error event threshold -- Maximum number of servers not responding	Specify the maximum number of servers that can be detected down before an error event is raised. The default is 10 servers.

ServerProcessesHigh

Use this Knowledge Script to monitor the number of Citrix Presentation Server or XenApp processes across all sessions. If the number of server processes exceeds the specified threshold, an event is raised.

Note
To gather data about all sessions on a specific Citrix server in a Citrix farm, run this Knowledge Script on that individual server in the farm.

This script returns the number of processes generated by all sessions on XenApp or Presentation Server. The event detail message includes information about each process, such as process name, process state, process ID, and username.

Processes not generated by Independent Computing Architecture (ICA) sessions are not considered.

Resource Object

Citrix Presentation Server object

Citrix XenApp object

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if number of processes exceeds the threshold?	Select **Yes** to raise an event if the number of XenApp or Presentation Server processes across all sessions exceeds the specified threshold. The default is Yes.
Event severity when number of processes exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Data Collection	
Collect data for number of processes?	Select **Yes** to collect data for charts and reports. If enabled, returns the number of XenApp or Presentation Server processes across all sessions. The default is unselected.
Monitoring	
Threshold -- Maximum processes on a server	Specify the maximum number of processes allowed on a server across all sessions before an event is raised. The default is 50 processes.

ServerProcessesResourceHigh

Use this Knowledge Script to monitor the use of CPU and memory resources by processes on Citrix Presentation Server or XenApp.

You can set thresholds for physical and virtual memory utilization and CPU utilization. If the use of resources by a process exceeds a threshold you set, an event is raised.

You can also set a script parameter to automatically terminate processes that exceed usage thresholds.

Resource Object

Citrix Presentation Server object

Citrix XenApp object

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if memory or CPU utilization exceeds threshold?	Select **Yes** to raise an event when the use of physical or virtual memory or CPU time exceeds the threshold you set. By default, events are enabled.
Event severity when memory or CPU utilization exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory or CPU utilization exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for memory and CPU utilization?	Select **Yes** to collect data for charts and reports. If enabled, returns information about the use of physical and virtual memory (in KB) and CPU time (as a percentage). The default is unselected.
Monitoring	
Threshold -- Maximum physical memory utilization	Specify the maximum amount of physical memory that can be used by any single XenApp or Presentation Server process before an event is raised. The default is 30720 KB.
Threshold -- Maximum virtual memory utilization	Specify the maximum amount of virtual memory that can be used by any single XenApp or Presentation Server process before an event is raised. The default is 61440 KB.
Threshold -- Maximum CPU utilization	Specify the maximum percentage of CPU time that can be used by any single XenApp or Presentation Server process before an event is raised. The default is 90%.

Description	How to Set It
Processes to monitor (comma-separated, no spaces)	Provide the names of the XenApp or Presentation Server processes you want to monitor. Separate multiple process names with commas and no spaces. For example, `Process1,Process2,Process3`. If no process names are entered, all processes are monitored. By default, all processes are monitored.
Terminate processes that exceed a threshold?	Select **Yes** to terminate any listed processes whose use of memory or CPU time exceeds the thresholds you set. The default is unselected.

ServerSessionsHigh

Use this Knowledge Script to monitor the number of sessions on Citrix XenApp or Presentation Server. If the number of sessions exceeds the threshold you set, an event is raised.

If data collection is enabled, this script returns the number of server sessions. The event detail message includes information about each session, such as session name, session ID, and username.

Resource Object

Citrix Presentation Server object

Citrix XenApp object

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if number of sessions exceeds threshold?	Select **Yes** to raise an event if the number of server sessions exceeds the threshold. The default is Yes.
Event severity when number of sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of sessions exceeds threshold. The default is 5.
Data Collection	
Collect data for number of sessions?	Select **Yes** to collect data for charts and reports. If enabled, returns the number of sessions, and information about each session. The default is unselected.
Monitoring	
Threshold -- Maximum number of sessions on a server	Specify the maximum number of sessions allowed on a server before an event is raised. The default is 20 sessions.

SessionPerUser

Use this Knowledge Script to monitor the number of sessions on Citrix XenApp or Presentation Server open for each user. You can monitor individual servers or entire server farms. If the number of sessions per user exceeds the threshold you specify, an event is raised.

Resource Object

Citrix Presentation Server object

Citrix XenApp object

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if number of sessions exceeds threshold?	Select **Yes** to raise an event if the number of user sessions exceeds the threshold you set. The default is Yes.
Event severity when number of sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of sessions exceeds the threshold you set. The default is 5.
Data Collection	
Collect data?	Select **Yes** to collect data for charts and reports. If enabled, returns the number of sessions on XenApp or Presentation Server open for each user. The default is unselected.
Monitoring	
Threshold -- Maximum number of sessions	Specify the maximum number of sessions on XenApp or Presentation Server that can be open for each user before an event is raised. The default is 5 sessions.
Monitor all servers in the farm?	Select **Yes** to monitor the number of sessions for all servers in a farm. The default is unselected.

SessionState

Use this Knowledge Script to monitor for Independent Computing Architecture (ICA) sessions that are in certain states. SessionState Knowledge Script can now monitor Citrix sessions per farm, generating event messages by farm name instead of server name.

If the number of sessions matching the states you select for monitoring falls below the minimum threshold or exceeds the maximum threshold you set, an event is raised.

SessionState obtains a list of all sessions from the Citrix XenApp API and loops through that list, looking at the state of each session. As an example, set the **Minimum threshold** to 2 and the **Maximum threshold** to 4. If this Knowledge Script finds two sessions in `LISTENING` state, and one in `ACTIVE` state, the number of sessions in `LISTENING` state is between the minimum and maximum thresholds, so the Knowledge Script will not raise an event for that state. The number of `ACTIVE` sessions has fallen below the minimum threshold, so the script raises an event for the `ACTIVE` state.

In a case like the one cited above, the Knowledge Script would not raise an event for any other session state, even if other states had fallen below the minimum threshold. It only raises events for a state if at least one session is in that particular state.

One use for this script is to track the number of active or idle XenApp or Presentation Server sessions.

Resource Object

Citrix Presentation Server object

Citrix XenApp object

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event when threshold exceeded or not met?	Select **Yes** to raise an event if the number of sessions matching a specified state exceeds or falls below the maximum or minimum threshold. The default is Yes.
Event severity when threshold exceeded or not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of sessions exceeds or falls below the threshold you set. The default is 5.
Data Collection	
Collect data for number of sessions in specified states?	Select **Yes** to collect data for charts and reports. If enabled, returns the number of sessions matching specified states. The default is unselected.
Monitoring	
Threshold -- Minimum number of sessions matching specified states	Specify the minimum number of sessions whose states must match the states you selected for monitoring before an event is raised. The default is 0 sessions (disabled).

Description	How to Set It
Threshold -- Maximum number of sessions matching specified states	Specify the maximum number of sessions whose states can match the states you selected for monitoring before an event is raised. The default is 5 sessions.
Session States to Monitor	
Session states that are monitored are as follows: • All session states • Active • Connected • Connecting • Disconnected • Down • Idle • Initializing • Listening • Resetting • Shadowing • Stale	Select **Yes** for each type of session state you want to monitor. By default, only **All session states** is set to Yes.

UserResourcesHigh

Use this Knowledge Script to monitor the utilization of CPU time and memory resources by users connected to XenApp or Presentation Server. You can select which users to monitor and set thresholds for physical or virtual memory utilization or CPU utilization.

Monitoring a user's processes occurs on a per-process basis. Resource utilization is only measured for the processes being used by the user selected for monitoring. However, the utilization metrics of different processes are not aggregated per user. All users on the server where you dropped the Knowledge Script are monitored by default.

If the percentage of CPU time or the amount of physical or virtual memory used by a process exceeds a threshold you set, an event is raised.

Resource Object

Citrix Presentation Server object

Citrix XenApp object

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event when CPU or memory utilization exceeds threshold?	Select **Yes** to raise an event when the use of CPU or memory resources by users connected to XenApp or Presentation Server exceeds any threshold you set. The default is Yes.
Event severity when CPU or memory utilization exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CPU or memory utilization exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for CPU and memory utilization?	Select **Yes** to collect data for charts and reports. If enabled, returns information about the use of CPU and memory resources by users connected to XenApp or Presentation Servers. The default is unselected.
Monitoring	
Threshold -- Maximum physical memory utilization	Specify the maximum amount of physical memory that can be consumed by users connected to XenApp or Presentation Server before an event is raised. The default is 30720 KB.
Threshold -- Maximum virtual memory utilization	Specify the maximum amount of virtual memory that can be consumed by users connected to XenApp or Presentation Server before an event is raised. The default is 61440 KB.

Description	How to Set It
Threshold -- Maximum CPU utilization	Specify the maximum percentage of CPU time that can be consumed by users connected to XenApp or Presentation Server before an event is raised. The default is 90%.
Users to monitor (comma-separated, no spaces)	Provide the names of the users you want to monitor. Separate names in a list with commas and no spaces (for example, `User1,User2,User3`). If no names are entered, all users are monitored. By default, all users are monitored.

Chapter 30
Dell OpenManage Knowledge Scripts

The AppManager for Dell OpenManage module provides the following Knowledge Scripts for monitoring Dell PowerEdge servers that run Dell OpenManage.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AdapterSCSI	Monitors the status of the Adapter SCSI subsystem on Dell servers.
AmperageProbe	Monitors the amperage level for a Dell server.
ArrayLogicalDrive	Monitors the status of the array logical drives on Dell servers.
ArrayPhysicalDrive	Monitors the status of the array physical drives on Dell servers.
EventLog	Monitors the Dell Embedded Systems Management (ESM) Event Log for system hardware errors or events.
FanProbe	Monitors the status of individual fans.
HealthCheck	Monitors all Dell server-related services.
MemCheck	Monitors the global status of the Dell memory devices.
NICError	Monitors network interface transmission errors.
NICFail	Monitors the status of the network interface.
PowerRedundancy	Monitors the redundancy status of Dell power supplies.
PowerSupply	Monitors the status of the Dell power supplies.
Report_AmperageProbe	Generates a report about the amperage levels for Dell servers.
Report_ArrayLogicalDrives	Generates a report about the status of the array logical drives on Dell servers.
Report_ArrayPhysicalDrives	Generates a report about the status of the array physical drives on Dell servers.
Report_FanProbe	Generates a report about the status of individual fans.
Report_NICErrorRate	Generates a report about network interface transmission errors.
Report_TemperatureProbe	Generates a report about the Dell server's thermal environment.
Report_VoltageProbe	Generates a report about the voltage levels for Dell servers.
TempProbe	Monitors the Dell server's thermal environment.
VoltageProbe	Monitors the voltage level for a Dell server.

AdapterSCSI

Use this Knowledge Script to monitor the status of the Adapter SCSI subsystem on Dell servers. If the subsystem is not operational, an event is raised. The Dell server defines the characteristics of normal operation, degraded operation, and subsystem failure.

Resource Object

Adapter SCSI icon

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the SCSI subsystem is operating properly. • **50** if the SCSI operation has degraded. • **0** if the SCSI subsystem has failed. The default is n.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community string you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`
Raise only one event if SNMP down?	Set to **y** to only raise a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity for SNMP or Dell Managed Node failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service or Dell Managed Node fails. The default is 10.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service has been restored. The default is 30.
Event severity when SCSI subsystem critical condition	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SCSI subsystem is in critical condition. The default is 10.
Event severity when SCSI subsystem degraded condition	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SCSI subsystem is in a degraded condition. The default is 20.

AmperageProbe

Use this Knowledge Script to monitor the amperage level for a Dell server. This Knowledge Script raises an event if the amperage drops below or exceeds the normal operating threshold. The Dell server defines the amperage levels for normal and degraded operation.

Resource Object

Amperage icon

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the amperage at each monitoring interval. The default is n.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community screen you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Raise only one event if SNMP down?	Set to **y** to raise only a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity for SNMP or Dell Managed Node failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which SNMP or Dell Managed Node fails. The default is 10.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service has been restored. The default is 30.
Event severity when amperage exceeded normal threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the amperage exceeded the normal threshold. The default is 10.
Event severity when amperage degraded	Set the event severity, from 1 to 40, to indicate the importance of an event in which the amperage is at a level for degraded operation. The default is 20.
Event severity when amperage not known or not monitored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the amperage is not known or not monitored. The default is 30.

ArrayLogicalDrive

Use this Knowledge Script to monitor the status of the array logical drives on Dell servers. This Knowledge Script raises an event if the drive is not operational. The Dell server defines the characteristics of normal operation, degraded operation, and logical drive failure.

Resource Object

Array Logical Drive icon

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the array logical drive is operating properly. • **50** if drive operation has degraded. • **0** if the array logical drive has failed. The default is n.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community screen you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Raise only one event if SNMP down?	Set to **y** to only raise a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity for SNMP or Dell Managed Node failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service or Dell Managed Node fails. The default is 10.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service has been restored. The default is 30.
Event severity when array logical drive failed	Set the event severity, from 1 to 40, to indicate the importance of an event in which the array logical drive fails. The default is 10.
Event severity when array logical drive degraded	Set the event severity, from 1 to 40, to indicate the importance of an event in which the array logical drive is in a degraded condition. The default is 20.
Event severity when array logical drive rebuilding or recovering	Set the event severity, from 1 to 40, to indicate the importance of an event in which the array logical drive is rebuilding or recovering. The default is 25.
Event severity when array logical drive offline	Set the event severity, from 1 to 40, to indicate the importance of an event in which the array logical drive is offline. The default is 25.

ArrayPhysicalDrive

Use this Knowledge Script to monitor the status of the array physical drives on Dell servers. This Knowledge Script raises an event if the drive is not operational. The Dell server defines the characteristics of normal operation, degraded operation, and physical drive failure.

Resource Object

Array Physical Drive icon

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the array physical drive is operating properly. • **50** if drive operation has degraded. • **40** if the array physical drive is rebuilding or recovering. • **0** if the array physical drive has failed or has been removed. The default is n.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community screen you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Raise only one event if SNMP down?	Set to **y** to raise only a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity for SNMP or Dell Managed Node failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service or Dell Managed Node fails. The default is 10.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service has been restored. The default is 30.
Event severity when array physical drive failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the array physical drive fails. The default is 10.
Event severity when array physical drive degraded condition	Set the event severity, from 1 to 40, to indicate the importance of an event in which the array physical drive is in a degraded condition. The default is 20
Event severity when array physical drive removed	Set the event severity, from 1 to 40, to indicate the importance of an event in which the array physical drive has been removed. The default is 15.
Event severity when array physical drive rebuilding or recovering	Set the event severity, from 1 to 40, to indicate the importance of an event in which the array physical drive is rebuilding or recovering. The default is 25.
Event severity when array physical drive offline	Set the event severity, from 1 to 40, to indicate the importance of an event in which the array physical drive is offline. The default is 25.

EventLog

Use this Knowledge Script to monitor the Dell Embedded Systems Management (ESM) Event Log for system hardware errors or events. This Knowledge Script raises an event for each new log entry since the previous iteration.

Resource Object

Dell Event Log

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Event?	Set to **y** to raise events. The default is y.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community screen you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Raise only one event if SNMP down?	Set to **y** to raise only a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity when SNMP or Dell Server Agent failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service or Dell Server Agent failed. The default is 9.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service has been restored. The default is 30.
Event severity when hardware events detected	Set the event severity, from 1 to 40, to indicate the importance of an event in which hardware events were detected. The default is 8.

FanProbe

Use this Knowledge Script to monitor the status of individual fans. This Knowledge Script raises an event for each fan being monitored that is not operating properly or if its status is unknown.

Resource Object

Dell Fan icon

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • The number of revolutions per minute (rpm) of the fan. • The status of the fan at each interval. If the fan status is monitored, the script returns a value of 1 if the fan is On, or a value of 0 if the fan is Off. The default is n.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community screen you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Raise only one event if SNMP down?	Set to **y** to raise only a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity for SNMP or Dell Managed Node failure	Set the event severity, from 1 to 40, to indicate the importance of on event in which the SNMP or Dell Managed Node failed. The default is 10.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of on event in which the SNMP service has been restored. The default is 30.
Event severity when fan critical	Set the event severity, from 1 to 40, to indicate the importance of on event in which the fan has a status of critical. The default is 10.
Event severity when fan degraded	Set the event severity, from 1 to 40, to indicate the importance of on event in which the fan is in a degraded status. The default is 20.
Event severity when fan not known or not monitored	Set the event severity, from 1 to 40, to indicate the importance of on event in which the status of the fan is not known or the fan is not monitored. The default is 20.

HealthCheck

Use this Knowledge Script to monitor all Dell server-related services. This Knowledge Script raises an event if any service is not running and automatically re-starts the stopped services. In addition, this Knowledge Script raises an event if SNMP is not operating or cannot get a MIB variable value.

Resource Objects

Dell server, any Dell Service icons

Default Schedule

The default interval is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Auto-start service?	Set to **y** to automatically restart the stopped services. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the status of Dell server-related services. The default is n.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community screen you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Event severity when service down; restart failed	Set the event severity, from 1 to 40, to indicate the importance of an event in which a service is down and restart failed. The default is 5.
Event severity when service down; restart succeeded	Set the event severity, from 1 to 40, to indicate the importance of an event in which a service is down and restart succeeded. The default is 25.
Event severity when service down; do not restart	Set the event severity, from 1 to 40, to indicate the importance of an event in which a service is down and will not be restarted. The default is 18.
Event severity when service down or cannot get MIB value	Set the event severity, from 1 to 40, to indicate the importance of an event in which the service is down or cannot get the MIB variable value. The default is 5.

MemCheck

Use this Knowledge Script to monitor the global status of Dell memory devices. This Knowledge Script raises an event if any memory device is not operational. The Dell server defines the conditions for normal operation internally.

Resource Object

Memory Check icon

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns the status of memory devices at each monitoring interval: • **100** if memory devices are operating properly. • **50** if operation has degraded. • **0** if memory devices have failed. The default is n.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community screen you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Raise only one event if SNMP down?	Set to **y** to raise only a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity for SNMP or Dell Managed Node failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service or Dell Managed Node failed. The default is 10.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service has been restored. The default is 30.
Event severity when memory device failed	Set the event severity, from 1 to 40, to indicate the importance of an event in which the memory device failed. The default is 10.
Event severity when memory device degraded	Set the event severity, from 1 to 40, to indicate the importance of an event in which the memory device has a status of degraded. The default is 20.
Event severity when memory device not known or not monitored.	Set the event severity, from 1 to 40, to indicate the importance of an event in which the condition of the memory device is not known or not monitored. The default is 30.

NICError

Use this Knowledge Script to monitor network interface transmission errors. This Knowledge Script reports both input and output errors and compares them to respective thresholds. This Knowledge Script raises an event if the number of network interface errors per minute exceeds the set threshold.

Resource Object

Dell Network Interface icon

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the operational status of the network interface subsystem at each monitoring interval. The default is n.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community screen you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Input errors per minute maximum threshold	Type a threshold for the maximum number of input errors per minute. The default is 2 errors per minute.
Output errors per minute maximum threshold	Type a threshold for the maximum number of output errors per minute. The default is 4 errors per minute.
Raise only one event if SNMP down?	Set to **y** to raise only a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity for SNMP or Dell Managed Node failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service or Dell Managed Node failed. The default is 9.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service has been restored. The default is 30.
Event severity when input errors per minute exceeded threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which input errors per minute exceeded the threshold. The default is 10.
Event severity when output errors per minute exceeded threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which output errors per minute exceeded threshold. The default is 10.

NICFail

Use this Knowledge Script to monitor the status of the network interface. This Knowledge Script checks whether the network interface subsystem is down when the administrator has indicated it should be in the **up** state. The event detail message includes the time at which the interface was discovered as **down**.

Resource Object

Dell Network Interface icon

Default Schedule

The default interval is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community screen you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns the operational status of the network interface subsystem at each monitoring interval. The default is n.
Raise only one event if SNMP down?	Set to **y** to raise only a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity for SNMP or Managed Node failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service or Managed Node failed. The default is 9.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service has been restored. The default is 30.
Event severity when network interface down	Set the event severity, from 1 to 40, to indicate the importance of an event in which the network interface is down. The default is 6

PowerRedundancy

Use this Knowledge Script to monitor the redundancy status of Dell power supplies. This Knowledge Script raises an event if power redundancy is not operational. The Dell server defines the characteristics of normal power redundancy, degraded redundancy, and redundancy failure.

Resource Object

Power Redundancy icon

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the redundant power supply is operating properly. • **50** if its operation has degraded. • **0** if the redundant power supply has failed. The default is n.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community screen you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Raise only one event if SNMP down?	Set to **y** to raise only a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity for SNMP or Dell Managed Node failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service or Dell Managed Node failed. The default is 10.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service has been restored. The default is 30.
Event severity when not redundant or status unknown	Set the event severity, from 1 to 40, to indicate the importance of an event in which the status of the power supply redundancy is not redundant or unknown. The default is 30.
Event severity when redundancy offline	Set the event severity, from 1 to 40, to indicate the importance of an event in which the status of the power supply redundancy is offline. The default is 20.
Event severity when redundancy degraded	Set the event severity, from 1 to 40, to indicate the importance of an event in which the status of the power supply redundancy is degraded. The default is 20.
Event severity when redundancy lost	Set the event severity, from 1 to 40, to indicate the importance of an event in which the status of the power supply redundancy is lost. The default is 10.

PowerSupply

Use this Knowledge Script to monitor the status of the Dell power supplies. This Knowledge Script raises an event if the power supply is not operational. The Dell server defines the status for normal, degraded, and failed operation.

Resource Object

Power Supply icon

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the power supply is operating properly. • **50** if its operation has degraded. • **0** if the power supply has failed. The default is n.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community string you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Raise only one event if SNMP down?	Set to **y** to raise only a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity for SNMP or Dell Managed Node failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service or Dell Managed Node failed. The default is 10.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service has been restored. The default is 10.
Event severity when power supply failed	Set the event severity, from 1 to 40, to indicate the importance of an event in which the power supply failed. The default is 10.
Event severity when power supply degraded	Set the event severity, from 1 to 40, to indicate the importance of an event in which the power supply has a status of degraded. The default is 20.

Report_AmperageProbe

Use this Dell_Report script to generate a report about the amperage levels for Dell servers. You can use this report to make a statistical analysis of the data point values over the time range you define for the report.

The AmperageProbe Knowledge Script collects data for this report.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Data source	
Select computers	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report. • **Minimum**: The minimum value of data points for the time range of the report. • **Maximum**: The maximum value of data points for the time range of the report. • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report. • **Range**: The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**: The measure of how widely values are dispersed from the mean. • **Sum**: The total value of data points for the time range of the report. • **Close**: The last value for the time range of the report. • **Change**: The difference between the first and last values for the time range of the report (close - open = change). • **Count**: The number of data points for the time range of the report.

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted. • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top%**: Chart only the top N% of selected data (sorted by default). • **Top N**: Chart only the top N of selected data (sorted by default). • **Bottom%**: Chart only the bottom N% of data (sorted by default). • **Bottom N**: Chart only the bottom N of selected data (sorted by default).
Percentage/count for top/bottom	Type a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column. • **Report Minimum**: The minimum value in a column. • **Report Maximum**: The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set the miscellaneous report properties.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Event severity for report success	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Event severity for report with no data	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity for report failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report failed to generate. The default is 5.

Report_ArrayLogicalDrives

Use this Dell_Report script to generate a report about the status of the array logical drives on Dell servers. You can use this report to make a statistical analysis of the data point values over the time range you define for the report.

The ArrayLogicalDrive Knowledge Script collects data for this report.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Data source	
Select computers	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report. • **Minimum**: The minimum value of data points for the time range of the report. • **Maximum**: The maximum value of data points for the time range of the report. • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report. • **Range**: The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**: The measure of how widely values are dispersed from the mean. • **Sum**: The total value of data points for the time range of the report. • **Close**: The last value for the time range of the report. • **Change**: The difference between the first and last values for the time range of the report (close - open = change). • **Count**: The number of data points for the time range of the report.

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted. • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top%**: Chart only the top N% of selected data (sorted by default). • **Top N**: Chart only the top N of selected data (sorted by default). • **Bottom%**: Chart only the bottom N% of data (sorted by default). • **Bottom N**: Chart only the bottom N of selected data (sorted by default).
Percentage/count for top/bottom	Type a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column. • **Report Minimum**: The minimum value in a column. • **Report Maximum**: The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set the miscellaneous report properties.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Event severity for report success	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Event severity for report with no data	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity for report failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report failed to generate. The default is 5.

Report_ArrayPhysicalDrives

Use this Dell_Report script to generate a report about the status of the array physical drives on Dell servers. You can use this report to make a statistical analysis of the data point values over the time range you define for the report.

The ArrayPhysicalDrive Knowledge Script collects data for this report.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Data source	
Select computers	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report. • **Minimum**: The minimum value of data points for the time range of the report. • **Maximum**: The maximum value of data points for the time range of the report. • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report. • **Range**: The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**: The measure of how widely values are dispersed from the mean. • **Sum**: The total value of data points for the time range of the report. • **Close**: The last value for the time range of the report. • **Change**: The difference between the first and last values for the time range of the report (close - open = change). • **Count**: The number of data points for the time range of the report.

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted. • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top%**: Chart only the top N% of selected data (sorted by default). • **Top N**: Chart only the top N of selected data (sorted by default). • **Bottom%**: Chart only the bottom N% of data (sorted by default). • **Bottom N**: Chart only the bottom N of selected data (sorted by default).
Percentage/count for top/bottom	Type a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column. • **Report Minimum**: The minimum value in a column. • **Report Maximum**: The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set the miscellaneous report properties.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Event severity for report success	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Event severity for report with no data	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity for report failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report failed to generate. The default is 5.

Report_FanProbe

Use this Dell_Report script to generate a report about the status of individual fans. You can use this report make a statistical analysis of the data point values over the time range you define for the report.

The FanProbe Knowledge Script collects data for this report.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Data source	
Select computers	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report. • **Minimum**: The minimum value of data points for the time range of the report. • **Maximum**: The maximum value of data points for the time range of the report. • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report. • **Range**: The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**: The measure of how widely values are dispersed from the mean. • **Sum**: The total value of data points for the time range of the report. • **Close**: The last value for the time range of the report. • **Change**: The difference between the first and last values for the time range of the report (close - open = change). • **Count**: The number of data points for the time range of the report.

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted. • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top%**: Chart only the top N% of selected data (sorted by default). • **Top N**: Chart only the top N of selected data (sorted by default). • **Bottom%**: Chart only the bottom N% of data (sorted by default). • **Bottom N**: Chart only the bottom N of selected data (sorted by default).
Percentage/count for top/bottom	Type a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column. • **Report Minimum**: The minimum value in a column. • **Report Maximum**: The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set the miscellaneous report properties.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Event severity for report success	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Event severity for report with no data	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity for report failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report failed to generate. The default is 5.

Report_NICErrorRate

Use this Dell_Report script to generate a report about network interface transmission errors. You can use this report to make a statistical analysis of the data point values over the time range you define for the report.

The NICError Knowledge Script collects data for this report.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Data source	
Select computers	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report. • **Minimum**: The minimum value of data points for the time range of the report. • **Maximum**: The maximum value of data points for the time range of the report. • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report. • **Range**: The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**: The measure of how widely values are dispersed from the mean. • **Sum**: The total value of data points for the time range of the report. • **Close**: The last value for the time range of the report. • **Change**: The difference between the first and last values for the time range of the report (close - open = change). • **Count**: The number of data points for the time range of the report.

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted. • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top%**: Chart only the top N% of selected data (sorted by default). • **Top N**: Chart only the top N of selected data (sorted by default). • **Bottom%**: Chart only the bottom N% of data (sorted by default). • **Bottom N**: Chart only the bottom N of selected data (sorted by default).
Percentage/count for top/bottom	Type a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column. • **Report Minimum**: The minimum value in a column. • **Report Maximum**: The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set the miscellaneous report properties.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Event severity for report success	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Event severity for report with no data	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity for report failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report failed to generate. The default is 5.

Report_TemperatureProbe

Use this Dell_Report script to generate a report about the Dell server's thermal environment. You can use this report to make a statistical analysis of the data point values over the time range you define for the report.

The TempProbe Knowledge Script collect data for this report.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Data source	
Select computers	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report. • **Minimum**: The minimum value of data points for the time range of the report. • **Maximum**: The maximum value of data points for the time range of the report. • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report. • **Range**: The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**: The measure of how widely values are dispersed from the mean. • **Sum**: The total value of data points for the time range of the report. • **Close**: The last value for the time range of the report. • **Change**: The difference between the first and last values for the time range of the report (close - open = change). • **Count**: The number of data points for the time range of the report.

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted. • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top%**: Chart only the top N% of selected data (sorted by default). • **Top N**: Chart only the top N of selected data (sorted by default). • **Bottom%**: Chart only the bottom N% of data (sorted by default). • **Bottom N**: Chart only the bottom N of selected data (sorted by default).
Percentage/count for top/bottom	Type a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column. • **Report Minimum**: The minimum value in a column. • **Report Maximum**: The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set the miscellaneous report properties.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Event severity for report success	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Event severity for report with no data	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity for report failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report failed to generate. The default is 5.

Report_VoltageProbe

Use this Dell_Report script to generate a report about the voltage levels for Dell servers. You can use this report to make a statistical analysis of the data point values over the time range you define for the report.

The VoltageProbe Knowledge Script collects data for this report.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Data source	
Select computers	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report. • **Minimum**: The minimum value of data points for the time range of the report. • **Maximum**: The maximum value of data points for the time range of the report. • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report. • **Range**: The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**: The measure of how widely values are dispersed from the mean. • **Sum**: The total value of data points for the time range of the report. • **Close**: The last value for the time range of the report. • **Change**: The difference between the first and last values for the time range of the report (close - open = change). • **Count**: The number of data points for the time range of the report.

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted. • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top%**: Chart only the top N% of selected data (sorted by default). • **Top N**: Chart only the top N of selected data (sorted by default). • **Bottom%**: Chart only the bottom N% of data (sorted by default). • **Bottom N**: Chart only the bottom N of selected data (sorted by default).
Percentage/count for top/bottom	Type a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column. • **Report Minimum**: The minimum value in a column. • **Report Maximum**: The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set the miscellaneous report properties.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Event severity for report success	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Event severity for report with no data	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity for report failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the report failed to generate. The default is 5.

TempProbe

Use this Knowledge Script to monitor the Dell server's thermal environment. If any component is operating out of normal temperature range, this Knowledge Script generates a warning event. If any component overheats beyond an acceptable temperature range, this Knowledge Script raises a critical condition event.

Resource Object

Temperature icon

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the temperature (in degrees Celsius) at each monitoring interval. The default is n.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community string you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Raise only one event if SNMP down?	Set to **y** to raise only a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity for SNMP or Dell Managed Node failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service or Dell Managed Node failed. The default is 10.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service has been restored. The default is 30.
Event severity when temperature critical	Set the event severity, from 1 to 40, to indicate the importance of an event in which the temperature condition is critical. The default is 10.
Event severity when temperature warning	Set the event severity, from 1 to 40, to indicate the importance of an event in which the temperature condition is warning. The default is 20.
Event severity when temperature not known or not monitored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the temperature is not known or not monitored. The default is 30.

VoltageProbe

Use this Knowledge Script to monitor the voltage level for a Dell server. This Knowledge Script raises an event if the voltage drops below or exceeds the normal operating threshold. The Dell server defines the voltage levels for normal operation.

Resource Objects

Voltage icon

Default Schedule

The default interval is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the voltage (in volts) at each monitoring interval. The default is n.
Community	Provide the SNMP community string required to access OpenManage resources. Provide the same community string you configured in AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Raise only one event if SNMP down?	Set to **y** to raise only a single event rather than an event for each monitored object when the SNMP service is down. The default is y.
Event severity for SNMP or Dell Managed Node failure	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service or Dell Managed Node failed. The default is 10.
Event severity when SNMP restored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the SNMP service has been restored. The default is 30.
Event severity when voltage level exceed critical threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the voltage level exceeded the critical threshold. The default is 10.
Event severity when voltage level near critical threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the voltage level is near the critical threshold. The default is 20.
Event severity when voltage not known or not monitored	Set the event severity, from 1 to 40, to indicate the importance of an event in which the voltage level is not known or not monitored. The default is 30.

Chapter 31
Diag Knowledge Scripts

The Diag category provides the following Knowledge Scripts for Diagnostic Console.

Most of the Knowledge Scripts for Diagnostic Console require no user interaction. These scripts are initiated on the selected AppManager server when you start AppManager Diagnostic Console. Do not change the parameter settings for these scripts — you will severely impact the data that Diagnostic Console collects. The one exception to the rule is StartCollectionAD, for which you can choose to enable the collection of Active Directory object counts.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
RetrieveData	Instructs the Diagnostic Console managed object to send all collected data back to the database.
StartCollectionAD	Instructs the Diagnostic Console managed object to collect data relating to Active Directory. In addition, enables or disables the collection of Active Directory object counts.
StartCollectionExchange	Instructs the Diagnostic Console managed object to collect data relating to Microsoft Exchange.
StartCollectionNT	Instructs the Diagnostic Console managed object to collect data relating to Microsoft Windows.

RetrieveData

The Knowledge Scripts for Diagnostic Console require no user interaction. This script is initiated on the selected AppManager server when you start AppManager Diagnostic Console.

RetrieveData tells the Diagnostic Console managed object to send all collected data back to the database.

Do *not* change the parameter settings for this script—you will severely impact the data that Diagnostic Console collects.

For more information about Diagnostic Console, see the *User Guide for Diagnostic Console*.

StartCollectionAD

StartCollectionAD tells the Diagnostic Console managed object to begin data collection on a domain controller for Diagnostic Console. In addition, you can choose to enable or disable the collection of Active Directory object counts. This Knowledge Script is initiated on the selected AppManager server when you start AppManager Diagnostic Console.

For more information about Diagnostic Console and this Knowledge Script, see the *User Guide for Diagnostic Console*.

Setting Parameter Values

Set the following parameter as needed:

Parameter	How To Set It
Collect database object count	By default, this script collects Active Directory object counts and displays them in the Database plug-in view of Diagnostic Console and in the Database report. The collection of this data causes a small increase in the overall CPU usage of the LSASS process. The increased usage is necessary for calculating the various object counts. To avoid the increased LSASS CPU load, you can disable the collection of object counts by setting this parameter to No. **Note** If you disable this parameter, the Object Counts table in the Database plug-in and Database report remains blank.

StartCollectionExchange

The Knowledge Scripts for Diagnostic Console require no user interaction. This script is initiated on the selected AppManager server when you start AppManager Diagnostic Console.

StartCollectionExchange tells the Diagnostic Console managed object to begin collecting data relating to Microsoft Exchange.

Do *not* change the parameter settings for this script—you will severely impact the data that Diagnostic Console collects.

For more information about Diagnostic Console, see the *User Guide for Diagnostic Console*.

StartCollectionNT

The Knowledge Scripts for Diagnostic Console require no user interaction. This script is initiated on the selected AppManager server when you start AppManager Diagnostic Console.

StartCollectionNT tells the Diagnostic Console managed object to begin collecting data relating to Microsoft Windows.

Do *not* change the parameter settings for this script—you will severely impact the data that Diagnostic Console collects.

For more information about Diagnostic Console, see the *User Guide for Diagnostic Console*.

Discovery Knowledge Scripts

The Discovery category provides Knowledge Scripts that discover information about your Microsoft Windows or UNIX operating environment and application-specific resource configuration. Each Discovery Knowledge Script has a specialized task, such as finding configuration details about the Windows operating system, the Microsoft Exchange Server, or the Microsoft SQL Server installed on the computer where you run the Knowledge Script.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ActiveDS	Discovers Active Directory servers and objects for Microsoft Windows 2000, Windows Server 2003, and Windows Server 2008.
AD-RT	Discovers ResponseTime for Active Directory clients.
AMHealth	Discovers AppManager and Control Center resources installed on Windows servers.
AMHealthUNIX	Discovers AppManager and Control Center resources installed on UNIX servers.
ApacheUNIX	Discovers the Apache resource and configuration information on UNIX servers.
AppAnalyzer	Discovers the AppAnalyzer Agent on an Exchange Server.
Application	Discovers a specified application (.exe or .com).
ARCserve	Discovers Computer Associates ARCserve servers and the services associated with them.
AvayaCM	Discovers Communication Manager resources and configuration information.
BackupExec	Discovers Symantec Backup Exec servers and the services associated with them.
BES	Discovers BlackBerry Enterprise Server v4.0 resource and configuration information.
BlackBerry	Discovers BlackBerry Enterprise Server resource and configuration information.
CallDataAnalysis	Discovers Call Data Analysis resource and configuration information.
CIM	Discovers resources associated with Compaq Insight Management Agents on Compaq servers.
CiscoCallMgr	Discovers Cisco CallManager configuration and resources.
CiscoCM	Discovers a Cisco Unified CallManager cluster and its resources.
CiscoCM_4x	Discovers a Cisco CallManager 4.x cluster and its resources.

Knowledge Script	What It Does
CiscoCME	Discovers Cisco CallManager Express configuration and resources, such as routers, switches, and gateways.
CiscoCNS_PerfE	Discovers the Cisco CNS Performance Engine (CNS-PerfE) and its configuration.
CiscoICD	Discovers Cisco ICD (Integrated Contact Distribution) configuration and resources.
CiscoICM	Discovers Cisco Intelligent Contact Management (ICM) configuration and resources.
CiscoICS	Discovers Cisco Integrated Communications System (ICS) configuration and resources.
CiscoIPTSecurity	Discovers security-related applications, such as Cisco Security Agent (CSA) and Symantec AntiVirus, on the Cisco IP telephony servers on which you installed the Cisco IP Telephony Security module.
CiscoIPTV	Discovers Cisco IP/TV configuration and resources.
CiscoIVR	Discovers Cisco Interactive Voice Response (IVR) configuration and resources.
CiscoPersonalAsst	Discovers Cisco Personal Assistant configuration and resources.
CiscoUE	Discovers Cisco Unity Express resources and configuration information.
CiscoUnity	Discovers Cisco Unity configuration and resources.
CiscoUnityBridge	Discovers Cisco Unity Bridge configuration and resources.
Cluster	Discovers clustered applications.
Dell	Discovers resources associated with Dell OpenManage/HIP capability on Dell servers.
Domino	Discovers Lotus Domino server configuration and resources, including partitioned servers.
Exchange	Discovers Microsoft Exchange Server 5.5 (or earlier) and Exchange 2000/2003 configuration and resources.
Exchange2007	Discovers configuration and resources for Microsoft Exchange Server 2007 or 2010.
ExchangeDAG	Discovers the virtual object for a Microsoft Exchange Server 2010 database availability group (DAG).
Exchange-RT	Discovers ResponseTime for Exchange clients and servers.
IIS	Discovers Microsoft Internet Information Server (IIS) configuration and resources.
MFXP	Discovers Citrix XenApp or Presentation Server resources and configuration information.
ModuleBuilder	Discovers configurations and resources for Module Builder
MOMReportAgent	Discovers the AppManager Reporting Agent. for MOM, which is installed with the XMP Report Module.
MQSeries	Discovers IBM MQSeries queues, queue managers, channels, and servers.
MSCS	Discovers Microsoft Cluster Server (MSCS) configuration and resources.

Knowledge Script	What It Does
NetBackup	Discovers Symantec NetBackup configuration and resources on Windows servers.
NetBackupUNIX	Discovers Symantec NetBackup configuration and resources on UNIX servers.
NetfinityDir	Discovers IBM Netfinity Director configuration and resources.
NetworkDevice	Discovers network device resources, such as routers, switches, host resources, and gateways.
NetWorker	Discovers Legato NetWorker servers and the services and other resources (such as backup groups and devices) associated with those servers.
Networks-RT	Discovers ResponseTime for Networks configuration and resources.
Networks-RTProxy	Discovers ResponseTime for Networks configuration and resources on remote computers (endpoints installed on UNIX computers and other places where a Windows-based AppManager agent and ResponseTime for Networks managed object are not installed).
NortelBCM	Discovers Nortel BCM (Business Communications Manager) configuration and resources.
NortelBCMx	Discovers the various components of a Nortel BCM installation for software version 4.0 and hardware models 50, 50a, 50e, 200, 400, and 1000.
NortelCC	Discovers Nortel Contact Center servers, databases, CDNs, DNISs, IVR queues, and IVR ports.
NortelCS	Discovers the various components of a Nortel CS1000 IP telephony system installation: Call Server, MGC, Signaling Server, NRS, MC32S, ECM, and VGMC.
NortelCS2x	Creates the Nortel CS2x supplemental database and configures the data collector services that collect data from Nortel CS2000 and CS2100 components.
NT	Discovers Microsoft Windows configuration and resource information.
OCS	Discovers all known resources on a Microsoft OCS server.
Oracle	Discovers configuration and resource information for Oracle Database servers.
Oracle-RT	Discovers ResponseTime for Oracle Database configuration and resources.
OracleUNIX	Discovers configuration and resource information for Oracle system resources installed on UNIX and Linux computers.
PhoneQuality	Discovers a Phone Quality object on the computer that will be used for monitoring IP phones.
ReportAgent	Discovers the NetIQ AppManager report agent and its data sources.
Security	Discovers Windows security resources on the computers in your network.
SharePoint	Discovers configuration and resource information for Microsoft SharePoint servers.
SharePoint2010	Discovers configuration and resource information for Microsoft SharePoint 2010 servers.

Knowledge Script	What It Does
Siebel	Discovers Siebel eBusiness Application components and resources on Windows computers.
Siemens	Discovers Siemens ServerView configuration and resources.
Snmp	Discovers SNMP devices on a network.
SQL	Discovers Microsoft SQL Server configuration and resources.
SQL-RT	Discovers ResponseTime for Microsoft SQL Server clients and servers.
StreamingMedia-RT	Discovers Streaming-RT configuration and resources.
UNIX	Discovers AppManager UNIX agents on managed UNIX servers.
VirtualCenter	Discovers VMware vCenter resources.
VoIPQuality_CallPerf	Discovers the VoIP Quality-Call Performance managed object when the AppManager agent, the managed object, and the Performance Endpoint are on the same computer.
VoIPQuality_CallPerfProxy	Discovers the VoIP Quality-Call Performance Proxy managed object on computer that does not have the AppManager agent installed but does have a NetIQ Performance Endpoint.
VoIPQuality_CallSetup_H.323	Discovers the H.323 protocol configuration and resources.
VoIPQuality_CallSetup_SIP	Discovers the SIP protocol configuration and resources.
VoIPQuality_CiscoSAA	Discovers the VoIP Quality-Cisco SAA managed object on a computer on which the Cisco SAA software is installed.
Web-RT	Discovers AppManager ResponseTime for Web resources, including Web sites, services, Web transactions, and related protocols.
WebLogicSvr	Discovers BEA WebLogic Application Servers installed on Windows servers.
WebLogicSvrUNIX	Discovers BEA WebLogic Application Servers installed on UNIX servers.
WebSphereAppSrv	Discovers WebSphere Application Servers and resources in the administrative domain.
WebSphereAppSrvUNIX	Discovers IBM WebSphere Application Servers and resources installed on UNIX servers.
WebSphereMQUNIX	Discovers IBM WebSphere MQ (formerly **MQSeries**) Servers on UNIX, including WebSphere MQ Server queues, queue managers, and channels.
Win-RT	Discovers AppManager ResponseTime for Windows resources. Verifies that a user domain, name, and password to be associated with the agent's Win-RT service have been entered in AppManager's Security Manager.
Win-RT7	Discovers settings for the ResponseTime 7.1 for Windows managed object and the ResponseTime for Windows service on Windows servers. It also verifies that the user domain, name, and password associated with the agent's ResponseTime for Windows service have been entered in AppManager Security Manager.
WMI	Discovers Microsoft Windows Management Instrumentation (WMI) server configuration and resources.
WS.NET	Discovers Web service resources and configuration for .NET on Windows computers.

Knowledge Script	What It Does
WTS	Discovers Microsoft Windows Terminal Server configuration and resources. If Citrix MetaFrame is installed on a Windows Terminal Server, this Knowledge Script discovers MetaFrame resources as well.
XenApp	Discovers Citrix XenApp resources and configuration information.

Discovering Application Resources

When you run a Discovery Knowledge Script on one or more computers, the Knowledge Script collects information about the resources (such as memory, CPU, physical disk space, etc.) on the selected computers and creates a view in the Operator Console for displaying these resources.

Once you have discovered an application's configuration on a computer, you can run additional application-specific Knowledge Scripts on that computer. For example, you need to run the NT Discovery Knowledge Script to get detailed information about the operating system on a computer before you can run any NT-specific Knowledge Scripts on that computer.

Rediscovering Application Resources

In most cases you discover applications by running an appropriate Discovery Knowledge Script with the schedule set to Run Once (which is the default). However, if you have frequent planned updates or other special circumstances, you may want to set an interval that corresponds to an application's update interval or change the default schedule to run multiple times.

This **rediscovery** process has some special characteristics that you should be aware of before you run a Discovery Knowledge Script on a previously discovered computer.

Rediscovering a computer enables you to update the configuration information stored in the AppManager repository and displayed in the Operator Console. If you rediscover a computer, there are three possible results:

- All of the same resource objects are discovered (nothing has been added or deleted)
- A new resource object is discovered (for example, maybe a new disk or disk partition has been added)
- A resource object that had been previously discovered is not discovered (for example, maybe a disk or disk partition has been removed)

Starting Jobs on Newly Discovered Objects

If all of the same resource objects are discovered, then the rediscovery has no impact on your AppManager jobs. However, if a new object is discovered and you have any jobs running against the folder under which the new object is added, the job does not automatically begin monitoring the new object.

To begin monitoring the new object, stop the job then drag and drop the Knowledge Script onto the folder to start a new job that includes the new object.

Stopping and Deleting Jobs on Obsolete Objects

If you know that a resource object has been removed, you should delete any existing jobs that run on the removed object before you run re-discovery. Otherwise rediscovery removes the object from the AppManager repository and the Operator Console, but any AppManager jobs that attempt to run against the object will return an error at each scheduled run.

To update the job with the correct object information:

- Stop and delete the existing job.
- Run the Discovery Knowledge Script to rediscover the objects.
- Drag and drop to start a new job that recognizes the current configuration.

Discovering Clustered Applications

When you add and discover clusters, you should only add real physical nodes to the TreeView. You should not add or discover virtual machines.

If you discover multiple nodes that are part of the same cluster, you may see what appear to be duplicate entries in the application view. For example, assume you have an Exchange Server cluster with the computers `LOBO1` and `LOBO2`. Both of these computers are displayed in the Master view. After you run the Exchange discovery to discover the cluster, `LOBO1` and `LOBO2` display the resource object `Exchange Server:LOSLOBOS_EXCH` in the Master view. `LOSLOBOS_EXCH` represents the virtual server. For example:

```
Master
  LOBO1
     CPU
     Memory
     Disk
     Network
     Exchange Server:LOSLOBOS_EXCH
  LOBO2
     CPU
     Memory
     Disk
     Network
     Exchange Server:LOSLOBOS_EXCH
```

In the TreeView, the physical node `LOBO1` is listed, along with all of its resource objects including the virtual Exchange Server. A similar list of resource objects is displayed for the physical node `LOBO2`.

If this is an active/passive Exchange Server cluster, after discovery in the Exchange view you would see two Exchange Server objects of `Exchange Server:LOSLOBOS_EXCH` that represent the virtual server `LOSLOBOS_EXCH` as viewed from the perspective of `LOBO1` and `LOBO2`, respectively.

```
Exchange
  Exchange Server:LOSLOBOS_EXCH
  Exchange Server:LOSLOBOS_EXCH
```

The first instance represents the virtual server when it is owned by the physical node `LOBO1` (that is, when `LOBO1` is the active server), and the second instance represents the virtual server when it is owned by `LOBO2`.

If this is an active/active Exchange Server cluster, the Master view displays `Exchange Server:LOBO_EXCH1` and `Exchange Server:LOBO_EXCH2` under `LOBO1`, and `EXCH Server:LOBO_EXCH1` and `EXCH Server:LOBO_EXCH2` under `LOBO2`.

```
Master
  LOBO1
     ...
     Exchange Server:LOSLOBOS_EXCH1
     Exchange Server:LOSLOBOS_EXCH2
  LOBO2
     ...
     Exchange Server:LOSLOBOS_EXCH1
     Exchange Server:LOSLOBOS_EXCH2
```

In the Exchange view, you would see two `Exchange Server:LOBO_EXCH1` objects and two `Exchange Server:LOBO_EXCH2` objects. They represent the same two virtual Exchange Servers as viewed from `LOBO01` and `LOBO02`, respectively. This duplication can apply for any clustered application.When you discover clustered applications such as Exchange and SQL Server, the discovered objects use the virtual server name (for example, `LOSLOBOS_EXCH` and `LOBO_EXCH1`). When you run the MSCS discovery, the discovered objects use the physical node name. For example, using the physical nodes and virtual server names described in the previous example, after running Discovery_MSCS, the Master view displays something similar to:

```
Master
  LOBO1
     ...
     MSCS Server:LOBO1
  LOBO2
     ...
     MSCS Server:LOBO2
```

What to Do When Discovery Fails

There are several reasons why a discovery job may fail. Some of the most common reasons discovery fails include:

- Network communication problems.
- The target computer does not have the applicable application or support software installed.
- The managed object has not been installed on the target computer.
- Required services, such as the AppManager agent or SNMP are not running on the computer you are discovering.
- Server-specific services such as the HP Systems Insight Management Agent or Dell HIP are not running on the computer you are discovering.
- A different login or community name is required to run the discovery on the target computer.

In many of these cases, you may see a severity 15 event and the short message displayed in the Event tab of the List pane indicates that the discovery is not applicable. For example, the message may display "Not a CIM server." If you see this type of event, check the event detail message for more specific information about what caused the discovery to fail. For example, the detail message may tell you that the community string name used was invalid. You then need to re-run the discovery with the correct community string name.

If more specific information is not available to help you track down the problem:

- Check that the AppManager agent services, Client Resource Monitor and Client Communication Manager, are installed and running on the target computer. You can use the **Services** Control Panel or run the **NT_RemoteServiceDown** Knowledge Script on the management server and list the target computers in the Machine List.
- Use the troubleshooting tool NetIQ Corporation Diagnostic Utility or other tools, such as NT_ServiceDown to verify SNMP is installed, running, and can get MIB variable values, if required (for example, if you are trying to discover hardware).
- Check that the appropriate managed object DLL has been installed on the computer.
- Check whether you have an appropriate login or community name if that information is required (this is server-specific; most Discovery Knowledge Scripts do not require special permissions or login accounts).

- Verify the application or server type of the computer and whether the version you are discovering is supported.

ActiveDS

Use this Knowledge Script to discover Active Directory servers and resources for Microsoft Windows 2000, Windows Server 2003, and Windows Server 2008. You can display the server name and the roles for the server, such as FSMO and Global Catalog.

Because the number of network computer objects stored in the Active Directory tree can be large, you can limit the number of Domain Naming Context and Configuration Container objects that are discovered:

- Specify the container level depth for discovery. Only container levels that are within the specified level of the domain tree are discovered.
- Specify the number of child objects to discover within a container level
- Specify the particular classes of objects you want to include or exclude for discovery. The option of selecting the objects to include or exclude, however, depends on which version of AppManager you are using.
- Specify whether to limit discovery to domains that have a direct trust relationship to the domain where discovery is performed; to domains that are in the same forest; or to Active Directory domains (to exclude Windows NT computers from discovery, for example).

Depending on the version of the AppManager agent on the Active Directory server, you can specify the objects you want by excluding or including them.

If the agent version is:	You can:
AppManager agent v5.0 (or earlier)	Limit the objects that are discovered by **excluding** particular classes from discovery. If you exclude a particular class, all objects are excluded. You cannot exclude specific instances of objects from within a class.
AppManager agent v5.0.1 (or later)	Limit the objects that are discovered by **including** particular classes in discovery. If you include a particular class, all objects are included. You cannot include specific instances of objects from within a class.

Resource Objects

Windows Server 2003 and Windows Server 2008 Active Directory servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_ActiveDS job fails. The default is 35 (magenta event indicator).

Discover Active Directory server resources

Description	How to Set It
Discover objects	
Use these parameters to determine which classes of objects are included in discovery and to set depth limits on the number of tree levels to discover. See Example of How This Knowledge Script Is Used for more information.	
Classes to include	Specify the class names you want to discover. Use commas with no spaces to separate more than one class. Enter class names as they appear in the Active Directory schema definition. If you include a particular class, all objects are included. You cannot include specific instances of objects from within a class. AppManager does not force discovery of the following classes: • container • organizationalUnit • server • serversContainer • site To discover these classes, you must specifically enter their names in this parameter. Include the organizationalUnit class to enable the monitoring of organizational units with the following Knowledge Scripts: • AD_NumberofComputers • AD_NumberofGroups • AD_NumberofObjects • AD_NumberofPrintQueues • AD_NumberofUsers • AD_NumberofUsersLocked Include the server class to discover and use the AD_ReplicationCheckByUSN Knowledge Script. The default is none (no classes specified).
Classes to exclude	Specify the names of classes you do not want to discover. This parameter is applicable only when running this script on an Active Directory server with Version 5.0 (or earlier) of the AppManager agent; this parameter is not applicable when running this script on an Active Directory server with Version 5.0.1 (or later) of the AppManager agent. Discovery information about Active Directory is required to run some AD Knowledge Scripts. Do not exclude the following classes: • container • computer • nTDSDSA • organizationalUnit • server • site • serversContainer Use commas with no spaces to separate the names of multiple classes. Specify class names as they appear in the Active Directory schema definition. The default is `user,group`. **Note** If you exclude a particular class, all objects are excluded. You cannot exclude specific instances of objects from within a class.

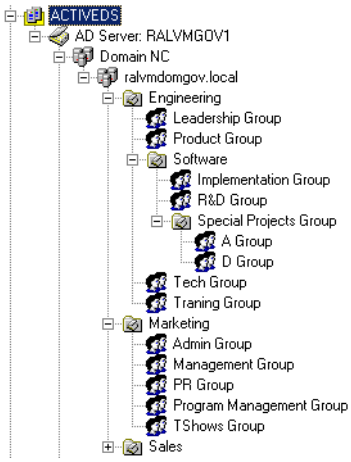
Description	How to Set It
Number of children per object	Specify the maximum number of child objects per container level to discover. Keep in mind that a child object can be another container. See "Example of How This Knowledge Script Is Used" on page 1531 for more information. Enter 0 to return all child objects for a container. The default is 5 child objects per container.
Number of levels deep to go in tree	Specify the maximum number of container levels deep in the domain object portion of the Active Directory tree to discover. To discover the child objects in a container, you must specify the level of the child object. See "Example of How This Knowledge Script Is Used" on page 1531 for more information. Enter 0 to return the complete tree structure. The default is 5 levels.
Discover domains and trusts?	Set to **Yes** to include the Domains and Trusts resource object in the Operator Console TreeView pane. If you enable this parameter, you can use the subsequent parameters to include or exclude types of domains from the Domains and Trusts resource object. The default is Yes.
Include only adjacent domains?	Set to **Yes** to limit discovery to domains that have a direct trust relationship to the servers where discovery is performed. By default, discovery is not limited to domains that have a direct trust relationship, and discovery walks transitive trusts within the forest.
Include only domains in forest?	Set to **Yes** to limit discovery to domains in the same forest as the servers where discovery is performed. The default is unchecked.
Include only Windows 2000 or later trusting domains?	Set to **Yes** to limit discovery to Active Directory domains that trust the domain of the server where discovery is performed (incoming trusts). Disable this parameter to include domains regardless of trust direction, including Windows NT domains and non-Windows domains. The default is Yes.
Event Notification	
Raise event if discovery succeeds?	Set to **Yes** to raise an event if discovery succeeds. The default is unchecked.
Event severity when discovery succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25 (blue event indicator).
Raise event if discovery fails?	Set to **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when discovery fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery fails. The default is 5 (red event indicator).
Raise event if discovery partially succeeds?	Set to **Yes** to raise an event if discovery returns some data but also generates warning messages. The default is Yes.
Event severity when discovery partially succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery returns some data but also generates warning messages. The default is 10 (red event indicator).
Raise event if discovery is not applicable?	Set to **Yes** to raise an event when discovery is not applicable. This type of failure usually occurs when the target computer does not have Active Directory installed or does not have the AppManager managed object for Active Directory. The default is Yes.
Event severity when discovery is not applicable	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery is not applicable. The default is 15 (yellow event indicator).

Description	How to Set It
Debug	
Save the discovery results file?	Set to **Yes** to save the discovery results to a file. The file is written to the `NetIQ\temp\netiq_debug` directory. The default is unchecked.

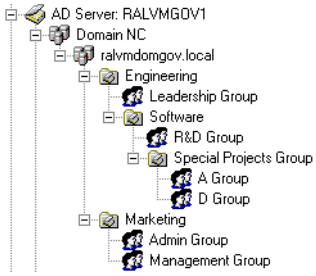
Example of How This Knowledge Script Is Used

When you discover Active Directory, the discovered Domain Naming Context and Configuration Container branches can potentially contain millions of objects. This script allows you to control the depth (in container levels) and width (in the number of child objects per container level) of the discovered branches. In addition, you can exclude all objects that belong to a specified class from discovery. By default, the Discovery_ActiveDS Knowledge Script discovers a minimal number of classes and objects. See ActiveDS for more information on the default settings and how to change them.

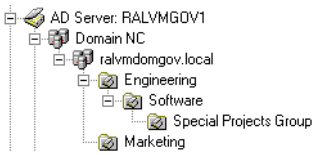
To illustrate how the these discovery parameters work, consider the following example. Assume the complete Domain NC tree has the following structure:



The container-level and children-per-object values are applicable to the containers and objects under `ralvmdomgov.local`. If the number of container levels is 0 (to discover all container levels) and the number of child objects per container level is 2, the discovery result might be similar to this:



To further control the number of objects returned, you can exclude particular classes. When you exclude a class, no instances of those objects are displayed. For example, if the “group” class is excluded from the discovery, the results of discovery might look something like this.



Note

The specific objects discovered when you use the *Number of children per object* and *Number of levels of the entire tree* parameters depends on how the ADSI enumerates the child objects.

AD-RT

Use this Knowledge Script to discover whether AppManager ResponseTime for Active Directory components are installed on a specific managed client. Drop this Knowledge Script on the managed client where you are performing discovery.

After successful discovery, a new object appears in the TreeView pane with a list of servers that support it. Also, a new AD-RT tab will appear in the Knowledge Script pane.

For information about using AppManager ResponseTime modules, see the corresponding AppManager ResponseTime *Management Guide*.

Resource Objects

Windows XP Professional, Windows 2000, or Windows NT.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can select the **Yes** check box to raise an event when the job succeeds. By default, events are not raised on success.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. This type of failure usually occurs when the target computer does not have all the prerequisites installed. The default is 10 (red event indicator).

AMHealth

Use this Knowledge Script to discover AppManager and Control Center resources installed on Windows servers. This Knowledge Script returns information about successful and failed discoveries, and it raises events to notify you of errors.

Notes

- If your Management Server is in a clustered environment, first run the Discovery_NT script on the nodes of the cluster for the Management Server to gather Windows operating system information for the Discovery_AMHealth script.
- Do *not* run the Discovery_NT script on the virtual server on which the Management Server is running.
- After running Discovery_NT, run Discovery_AMHealth on the nodes of the cluster for the Management Server.
- For more information about working with a Management Server in a clustered environment, contact NetIQ Professional Services for a Technical Reference on that topic.

Configuring Security Manager for Discovery_AMHealth

If an agent is not installed on the QDB, and the NetIQ Client Resource Monitor (`netiqmc`) or Client Communication Manager (`netiqccm`) service accounts on the Management Server do not have sufficient rights to access the QDB, configure the NetIQ services with a Windows account that has access to the QDB. Otherwise, you need to configure the Knowledge Script to use SQL authentication.

If an agent is not installed on the Control Center repository (NQCCDB), and the `netiqmc` or `netiqccm` service accounts on the NetIQ Command Queue Server do not have sufficient rights to access the NQCCDB, configure the NetIQ service accounts with a Windows account that has access to the NQCCDB. Otherwise, you need to configure the Knowledge Script to use SQL authentication.

If the service account does not have sufficient privileges before running Discovery_AMHealth, set up SQL authentication with AppManager Security Manager.

To configure Security Manager for Discovery_AMHealth:

1. On the Extensions menu in the Operator Console, click **Security Manager**.
2. Connect to the QDB.
3. Expand **Computers** and select the Management Server from the list of computers.
4. On the Custom tab, click **Add**.
5. In the Label field, type `sql$<management server name>`. For example, if your Management Server name is SERVER1TEST, you would type `sql$SERVER1TEST`.
6. In the Sub-Label field, type a SQL user name that exists in the QDB.
7. In the Value 1 field, type the password for the user entered in the Sub-Label field.
8. Select **Extended application support** to encrypt the password when it is stored in the repository.
9. Click **OK**.

10. Click **Apply** to save the changes.

Note
When you want to discover the Management Server, type the SQL user name from step 6 of this procedure into the *SQL Server login* parameter of the Discovery_AMHealth Knowledge Script.

Resource Objects

Windows servers running AppManager

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise an event if discovery succeeds?	Select **Yes** to raise an event when discovery succeeds. The default is unselected.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which when the discovery succeeds. The default is 25.
Raise event if discovery fails?	Select **Yes** to raise an event when discovery fails. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the discovery fails. The default is 5.
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_AMHealth job itself fails. The default is 35.
SQL Server login	Specify the SQL user name required for access to the AppManager repository (QDB). Leave this field blank to use Windows NT authentication. **Note** If you want to use a specific SQL Server login account, use Security Manager to update the AppManager repository with the SQL Server logins that you want to use. For more information, see the *Installation Guide* for AppManager.

AMHealthUNIX

Use this Knowledge Script to discover AppManager and Control Center resources installed on UNIX servers. This Knowledge Script returns information about successful, failed, and partial discoveries, and it raises events to notify you of errors.

Resource Objects

UNIX servers running AppManager

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if discovery succeeds?	Set to **y** to raise an event when discovery succeeds. The default is n.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance when the discovery fails. The default is 5.
Event severity when discovery partially succeeds.	Set the event severity level, from 1 to 40, to reflect the importance when the discovery partially succeeds. This type of situation usually occurs when the target computer does not have all the prerequisites installed. The default is 15.

ApacheUNIX

Use this Knowledge Script to discover Apache Web servers installed on UNIX servers. This Knowledge Script returns information about successful, failed, and partial discoveries and raises events (with user-specified severity) to notify you of errors.

This Knowledge Script may be used to determine if and where Apache Web servers are installed in a UNIX network. Run this Knowledge Script periodically to detect new instances of Apache Web servers and to determine whether existing servers have been uninstalled or taken offline.

Resource Object

UNIX computer with Apache Web Server

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	Set to **y** to raise an event when the Knowledge Script discovers an Apache Web server. The default is n.
Event severity when Discovery succeeds?	Specify a severity level for the event raised by successful discovery of an Apache Web server. The default is 25.
Event severity when Discovery fails?	Specify a severity level for the event raised by failure to discover an Apache Web server. The default is 5.
Event severity when Discovery is partially done?	Specify a severity level for the event raised when the Knowledge Script starts but does not run to completion. The default is 10.
Event severity when Discovery is not appropriate?	Specify a severity level for the event raised when the Knowledge Script cannot discover Apache Web servers. This occurs when no servers are installed, or when you try to run the Knowledge Script in a network where no UNIX servers are running. The default is 15.
Semi-colon separated list of paths to search for the Apache binary program	Use this variable to expedite the discovery process. Specify a list of directory paths (semi-colon delimited). The Knowledge Script will limit its search for the Apache binary program to the paths you specify. The default is \usr.

AppAnalyzer

Use this Knowledge Script to discover the AppAnalyzer Agent.

Resource Objects

Any Exchange server hosting an AppAnalyzer Agent.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery? (y/n)	Set to **y** to raise an event if the AppAnalyzer Agent is successfully discovered. The default is y.
Event severity when discovery...	Set the event severity level, from 1 through 40, to indicate the importance of the event when discovery: • **...succeeds**. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. The Knowledge Script returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have the AppAnalyzer Agent installed. The default is 15 (yellow event indicator).

Application

Use this Knowledge Script to discover user-specified applications and set the event notification level you want to see based on discovery status. With this Knowledge Script, you can have AppManager discover applications you want to monitor by entering the path to the application executables. This allows you to monitor your own internally developed applications or commercial applications not currently supported through the AppManager suite.

Resource Objects

User-defined applications.

Default Schedule

By default, this Knowledge Script is only run **once** for each computer. If you have frequent planned updates to the specified applications on particular computers, you can set an interval that corresponds to the application's update interval.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery? (y/n)	Specify whether you want to raise an event when the job succeeds. This Knowledge Script always raises an event when the job fails for any reason. The default is n.
Full path to executable (separated by commas with no spaces)	Type the absolute path to the executable you want to discover on the target computer. You can enter multiple executables, separated by commas. For example: `C:\Program Files\cpro.exe,D:\MyGames\golf.exe`.
Event severity if discovery...	Set the event severity level, from 1 through 40, to reflect the importance if the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator).
View name of the discovery	Type the name you want displayed in the View tab for the application(s), for example `Oracle,MyApp`. When you discover an application, a new application view is created in the Operator Console. The default is `Application`.
Version of the application	Type the version of the application you are discovering. This version information is then available in the Operator Console when you look up a computer's properties (right-click on the computer in the TreeView and choose **Properties**). The default is * (asterisk), all versions.

Example of How this Knowledge Script Is Used

If you have in-house, high-volume, or mission-critical applications such as an Accounts Payable program or a internal customer relations application that you want to monitor and gather statistics for, you can use this Knowledge Script to add the application to your Operator Console's monitoring environment.

Once discovered, you can use the Application Knowledge Scripts to perform routine monitoring tasks such as checking whether the application is up or the CPU usage is high, or develop your own custom Knowledge Scripts to perform more application-specific activities.

ARCserve

Use this Knowledge Script to discover Computer Associates ARCserve servers and the services associated with them.

Resource Objects

ARCserve servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25. • **...fails**. The default is 10. • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 20.

AvayaCM

Use the Discovery_AvayaCM Knowledge Script to discover Avaya Communication Manager configuration information and resources, including Switch Processing Elements (SPE), Enterprise Survivable Servers (ESS), Local Survivable Processors (LSP), H.248 media gateways, IP stations, attendant consoles, and remote office stations. You can also choose to discover NetIQ SNMP Trap Receiver.

Prerequisite

AppManager uses SNMP queries to access remote Communication Manager servers and to enable the functionality of NetIQ SNMP Trap Receiver. Before discovering Communication Manager resources, enter SNMP community string information into AppManager Security Manager.

Configuring Community Strings for Remote Communication Managers

Configure SNMP community string information for each Communication Manager you want to monitor. On the Custom tab in Security Manager, complete the following fields:

Field	Description
Label	`SNMP`
Sub-label	Indicate whether the community string information will be used for a single device or for all devices: • *For a single Communication Manager*, type <*`device IP address`* or *`hostname`*>. The address or hostname must match the address or hostname you provide in the parameters for the Discovery_AvayaCM Knowledge Script. • *For all Communication Managers*, type `default`.
Value 1	The appropriate read-only community string value, such as `private` or `public`.

Configuring Community Strings for Trap Receiver Functionality

Configure SNMP community string information for each Trap Receiver device that will send traps to the proxy agent computer. On the Custom tab in Security Manager, complete the following fields:

Field	Description
Label	`SNMPTrap`
Sub-label	Provide the IP address or hostname of the device on which Trap Receiver is installed. **Note** If you have already run the Discovery_AvayaCM Knowledge Script, use the same IP address or hostname that is displayed for the AvayaCM object in the TreeView.
Value 1	Provide the community string name included in each trap sent by Trap Receiver, such as `private` or `public`.

Resource Object

Windows server

Only one computer can act as proxy for any given Communication Manager cluster. Therefore, run this script on only one computer at a time.

Default Schedule

By default, this script runs weekly, on Sunday at 2 PM.

Setting Parameter Values

Set the parameters on the Values tab as needed

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of the failure of the Discovery_AvayaCM job. The default is 5.
Set up supplemental database?	Select **Yes** to create the Avaya CM supplemental database, including the tables and stored procedures needed to store call detail records and phone deregistration information. The default is Yes.
Event severity when database setup fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Avaya CM supplemental database is not created. The default is 15. It is possible that the supplemental database was not created because the Discovery job ran on a computer on which SQL Server is not installed.
Start pruning job on supplemental database?	**For all supported versions of SQL Server, except SQL Server 2005 Express**: Set to **Yes** to create a SQL job that deletes data from the supplemental database. The SQL job runs every night. Data is deleted from the supplemental database based on the value you specify in the *Number of days to keep call detail records* parameter. The default is Yes. **For SQL Server 2005 Express**: Set to **No**. The pruning job is not supported for SQL Server 2005 Express. **To manually delete data from the supplemental database**: 1. Run the following stored procedure from a command line: `osql -E -S <sql server> -n -d <database> -Q "exec dbo.Task_AvayaCM_Pruning"` where `<sql server>` is the name of the server that hosts the supplemental database, and where `<database>` is the name of the supplemental database. For example: `osql -E -S SuppDBAvaya -n -d AvayaCM_S8300-Cluster -Q "exec dbo.Task_AvayaCM_Pruning"` 2. Configure a Windows Scheduled Task to schedule pruning at an interval of your choosing. The process for configuring a Windows Scheduled Task varies according to your version of Microsoft Windows. Consult your Windows documentation for more information.
Number of days to keep call detail records	Specify the number of days' worth of CDRs to keep in the Avaya CM supplemental database. Data older than what you specify is discarded. The default is 7 days.

Parameter	How to Set It
Local SQL Server Instance name	Specify the name of the local SQL Server instance (on the proxy computer) in which you want to create the new Avaya CM supplemental database. Leave this parameter blank to accept the default name.
Raise event if database setup succeeds?	Select **Yes** to raise an event if creation of the Avaya CM supplemental database is successful. The default is unselected.
Event severity when database setup succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Avaya CM supplemental database is created successfully. The default is 25.
SNMP	
Global SNMP Message timeout	Specify the number of seconds discovery should attempt an SNMP message request to an *individual* Communication Manager server before retrying the connection. The default is 120 seconds. The value you set here is the timeout value for *all* SNMP message requests for *all* AvayaCM Knowledge Script jobs.
Global SNMP Task timeout	Specify the number of seconds discovery should attempt an SNMP retrieve request to an *individual* Communication Manager server before retrying the connection. The default is 3600 seconds. The value you set here is the timeout value for *all* SNMP retrieve requests for *all* AvayaCM Knowledge Script jobs.
Global SNMP retries	Specify the number of times discovery should attempt an SNMP connection to an individual Communication Manager before attempting an SNMP connection to the next Communication Manager in the list. The default is 4 retries. The value you set here will be the number of retries for *all* SNMP connections for *all* AvayaCM Knowledge Script jobs. **Hint** If you experience timeouts that appear to be caused by lost messages rather than CPU usage, increase the number of retries, which affects SNMP `GETNext` and `GETBulk` requests. For example, if CPU is stable and you have already increased the timeout value, but packet loss in the network is high and timeouts are still being experienced, you can increase the number of retries.
Enable use of SNMP GETBulk requests during discovery?	By default, this parameter is enabled, allowing the Discovery_AvayaCM Knowledge Script job to use SNMP `GETNext` and `GETBulk` requests to access Communication Manager MIBs. Disable this parameter to allow the script to use only `GETNEXT` requests. Not all MIB tables are extensive enough to need a `GETBulk` request. A `GETBulk` request is faster, but more CPU-intensive than a `GETNext` request.
Number of rows to request for each GETBulk operation	Specify the number of rows from the MIB table to return in a `GETBulk` request. The default is 10 rows. The number of rows determines how quickly MIB data is returned. If CPU usage is too high, you can reduce the number of rows per `GETBulk` request or disable the *Enable use of SNMP GETBulk requests during discovery?* parameter.
Interval to pause between GETBulk requests	Specify the number of milliseconds to wait between GETBulk requests. The default is 100 milliseconds. The delay can help manage CPU usage and speed of SNMP requests. For example, a one-row `GETBulk` with a 100-millisecond delay between requests executes slower and uses less CPU than a `GETNext` request.
Raise event if discovery succeeds?	Select **Yes** to raise an event if discovery succeeds in finding Communication Manager devices. The default is unselected.

Parameter	How to Set It
Event severity when discovery succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds in finding Communication Manager devices. The default if 25.
Raise event if discovery fails?	Select **Yes** to raise an event if discovery fails to find some or all of your Communication Manager devices. The default is Yes.
Event severity when discovery fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery fails to find some or all of your Communication Manager devices. The default is 10.
Discover Avaya Communication Manager Servers	
Discovery timeout for all servers	Specify the number of minutes the script should attempt to discover *all* specified Communication Manager servers before stopping as unsuccessful. The maximum is 60 minutes. The default is 30 minutes.
Maximum number of concurrent discoveries	Specify the maximum number of Communication Manager servers that can be queried for discovery at one time. No matter what value you enter, discovery is still performed for the entire list of devices that you specify in the following parameters. Setting this parameter to a low value throttles the number of SNMP requests performed at one time, but may increase the overall time it takes to discover a list of devices. The default is 10 concurrent discoveries.
Comma-separated list of active Communication Manager servers	Use this parameter if you know which Communication Manager servers you want to discover. Specify at least one IP address or hostname, using a comma to separate multiple items. For example: `10.0.1.1,10.0.1.7` You can enter IP addresses or hostnames, but you *must* enter the same IP address or hostname for which you configured SNMP community string information. If you configured a community string for a hostname, enter the *same* hostname; if you configured an IP address, enter the *same* IP address.

Comma-separated list of Communication Manager IP address pairs in a single NAT cluster	MSPs (Managed Service Providers) frequently maintain distributed customer networks in which NAT (Network Address Translation) is used to translate the IP address ranges that are monitored from a single NOC (Network Operations Center). The use of NAT prevents AppManager from recognizing the actual IP addresses of the servers in the remote cluster. If your AppManager agent is located on a server in the NOC, but the monitored devices are located in a cluster in the remote customer network, you need to provide AppManager with a list of the IP addresses of the remote monitored devices.
	Use this parameter to enable AppManager to recognize the IP addresses of the servers for a single remote Communication Manager cluster.
	Type a list of IP address pairs for the Communication Manager servers in a remote cluster. Use commas to separate the addresses. A pair consists of a server's NAT (external) IP address and its IP address inside the cluster. A Communication Manager cluster can contain three IP addresses: an active SPE virtual address, a primary physical address, and a secondary physical address. Each of these addresses must be represented by a pair in this parameter. A maximum of six IP addresses is allowed in this parameter.
	Use the following format:
	`externalactiveSPEvirtualaddress,internalactiveSPEvirtualaddress,externalprimaryphysicaladdress,internalprimaryphysicaladdress,externalsecondaryphysicaladdress,internalsecondaryphysicaladdress`
	In the following example, the 10.41* addresses are externally visible and the 172.16* addresses are visible only to the Communication Managers:
	`10.41.1.10,172.16.1.10,10.41.1.11,172.16.1.11,...`

Parameter	How to Set It

Full path to file with list of active Communication Manager servers	Instead of listing each server separately, you can specify the full path to a file on the proxy computer that contains a list of IP addresses or hostnames of Communication Manager servers.
	In the file, specify the servers on multiple lines and ensure that each line contains only one entry. For example:
	`AvayaCM01`
	`AvayaCM02`
	`AvayaCM10`
	You can enter IP addresses or hostnames, but you *must* enter the same IP address or hostname for which you configured SNMP community string information. If you configured a community string for a hostname, enter the *same* hostname in the list; if you configured an IP address, enter the *same* IP address in your list.

Discover Trap Receiver?	Select **Yes** to discover NetIQ SNMP Trap Receiver. The default is unselected.
Trap Receiver IP address	Specify the IP address of the computer on which Trap Receiver is installed. The default is `localhost`.
Trap Receiver TCP port	Specify the TCP port number through which Trap Receiver will communicate with AppManager. The default is port 2735.
Configure Trap Receiver for associated servers?	Select **Yes** to allow Trap Receiver to listen for traps coming from other servers such as SIP Enablement Services (SES) servers or Application Enablement Services (AES) servers. The default is unselected.
Comma-separated list of associated server IP addresses	Provide a comma-separated list of the IP addresses of other servers. If you enabled the *Configure Trap Receiver for associated servers?* parameter, then Trap Receiver will listen for traps coming from the servers you specify.

BackupExec

Use this Knowledge Script to discover Symantec Backup Exec servers and the services associated with them.

Resource Objects

Backup Exec servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have Backup Exec installed. The default is 15 (yellow event indicator).

BES

Use this Knowledge Script to discover BlackBerry Enterprise Server (BES) 4.0 (and higher) configuration and resources.

For earlier versions of BlackBerry Enterprise Server, use the BlackBerry Knowledge Script.

Prerequisite

To discover BES resources and run BES Knowledge Scripts, you must configure your SNMP community string information in AppManager Security Manager.

Security Manager keeps community-string and password information secure and private. Instead of getting the information from a Knowledge Script parameter, the Knowledge Scripts get this information automatically and securely from Security Manager.

On the Custom tab in Security Manager, complete the following fields for every agent computer you want to monitor with AppManager for BlackBerry Enterprise Server:

Field	Description
Label	BESSNMP$<*name of BES server on which you installed the module*>
Sub-label	`community`
Value 1	Read-only community string, such as `private` or `public`

Resource Object

BlackBerry Enterprise Server 4.0.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event when monitoring fails. Default is 40 (magenta event indicator).
Raise event if discovery succeeds?	Select the **Yes** check box to raise events when discovery succeeds. By default, events are enabled.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue event indicator).
Raise event if discovery fails?	Select the **Yes** check box to raise events when discovery fails. By default, events are enabled.

Parameter	How to Set It
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).
Raise event if AppManager for BlackBerry Enterprise Server 4.0 managed object not installed?	Select the **Yes** check box to raise an event if the managed object for AppManager for BlackBerry Enterprise Server 4.0 is not installed on the selected computer(s). By default, events are enabled.
Event severity when AppManager for **BlackBerry Enterprise Server 4.0** managed object not installed	Set the event severity level, from 1 to 40, to indicate the importance of the event when the managed object cannot be found. The default is 15 (yellow event indicator).

BlackBerry

Use this Knowledge Script to discover BlackBerry Enterprise Server resource and configuration information.

Resource Objects

BlackBerry Enterprise Servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 through 40, to indicate the importance of the event when discovery: • **...succeeds**. The default is 25. • **...fails**. The default is 5. • **...is partially done**. The Knowledge Script returns some data but also generates warning messages. The default is 10. • **...is not applicable**. This type of failure usually occurs when the target computer does not have the AppManager for Blackberry Enterprise Server component installed. The default is 15.

BlackBerry-Domino

Use this Knowledge Script to discover Research In Motion (RIM) BlackBerry Enterprise Server for Lotus Domino resources and configuration information. You can specify unique events indicating that the servers are discovered fully or partially, or if discovery fails. The Knowledge Script raises an event if the job fails for any reason.

Resource Objects

BlackBerry Enterprise Server for Lotus Domino.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery? (y/n)	Specify whether you want to raise an event if a server is discovered fully or partially. This Knowledge Script always raises an event if discovery fails. The default is n.
Event severity level if discovery...	Set the event severity level, from 1 through 40, to indicate the importance of the event: • **... succeeds**. The default is 25 (blue event indicator). • **... fails**. The default is 5 (red event indicator). • **... is partially done**. The default is 10 (red event indicator). • **... is not applicable**. The default is 15 (yellow event indicator).

Brocade (BRCD)

Use this Knowledge Script to discover your Brocade switches.

Resource Objects

Computer running the Brocade proxy.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Switch User Name	Supply the username you created for the Brocade switches from the Fabric View. All switches using the same proxy must use the same User Name. This value is encrypted and appears in this field as asterisks. If you supplied the username and password in the Security Manager, you do not need to specify it here. If you specify User Name information in both places, these parameters supersede the Security Manager for switch discovery.
Switch User Password	Supply the password for this User ID. This value is encrypted and appears in this field as asterisks.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have Brocade proxy application installed. The default is 15 (yellow event indicator).

CallDataAnalysis

Use this Knowledge Script to discover Call Data Analysis resource and configuration information in the TreeView pane of the Operator Console.

Resource Objects

NT_MachineFolder

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
SQL Data Warehouse Access	
Note The data warehouse is a database that is created within SQL Server when you install the Call Data Analysis module. The data warehouse provides the central view of the collected data, and has links to the data mart databases.	
SQL user name (leave blank for Windows authentication)	Enter the SQL user name required for access to the data warehouse computer. Leave this field blank to use Windows NT authentication. **Note** If you want to use a specific SQL Server login account, use Security Manager to update the AppManager repository with the SQL Server logins that you want to use. For more information, see the *Installation Guide* for AppManager.
Event Notification	
Raise event if discovery succeeds?	This Knowledge Script always raises an event when discovery fails. Set to **Yes** to raise an event when discovery is successful. The default is unchecked.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of successful discovery.
Raise event if discovery partially succeeds?	This Knowledge Script always raises an event when discovery fails. Set to **Yes** to raise an event when discovery is partially successful. The default is Yes.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance when discovery is partially successful. The default is 15.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance when discovery fails. The default is 5.

CIM

Use this Knowledge Script to discover Hewlett-Packard Systems Insight Manager (SIM) configuration and resources. This Knowledge Script requires SNMP and the SIM Agent to be running on the computer you are discovering. If a required service is not found or is not running, the Discovery job fails with a "Not a CIM server" event.

Systems Insight Manager was formerly known as Compaq Insight Manager.

Resource Objects

CIM servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
SNMP community string	Enter the SNMP community name to use. The default is the community name entered in the AppManager Security Manager or public if no community name has been entered.

Parameter	How to Set It
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have CIM installed. The default is 15 (yellow event indicator). **Note** If required services, such as SNMP or the Compaq Insight Management Agent, are not running on the computer you are discovering, you may see a severity 15 event (Not a CIM server). If you see this type of event, see the detail message for more information about what caused discovery to fail.
Discover only physical interfaces?	Select **Yes** to only discover interfaces that are associated with a NIC card. Microsoft Windows Server 2008 and Microsoft Windows Server 2008 R2 provide virtual interfaces, which are interfaces that are not associated with a NIC card. If you set this parameter to no, AppManager displays virtual as well as physical interfaces in the TreeView. However, CIM_NICFail and CIM_NICError Knowledge Scripts are only applicable to physical interfaces. If you attempt to run these Knowledge Scripts on virtual interfaces, the jobs will report errors. If you set this parameter to yes, the console TreeView pane shows extra objects as null or unidentified. The objects do not cause errors or problems with how the module works. Any time you change this parameter setting, you must recreate all CIM_NICFail and CIM_NICError jobs on Windows Server 2008 and Windows Server 2008 R2 computers. The default is yes, which results in no discovery of virtual interfaces.

CiscoCallMgr

Use this Knowledge Script to discover Cisco CallManager configuration and resources.

Prerequisite

Discover Windows resources on the server that you want to monitor *before* you discover CallManager resources. If you have not yet discovered Windows resources, run the NT discovery Knowledge Script.

Understanding stiBack Version Numbers

Discovery_CiscoCallMgr retrieves the stiBack version number from the registry. If no backup has ever been run, the version number in the registry contains a "0" as its third number, for example: 3.1.0.39. However, if you were to look at **Help > About** for the stiView applet, you would not see the "0." To continue the example, you would see 3.1.39. Once you run a backup, the version number in the registry will match the version number in **Help > About**. Then, the next time CallManager discovery runs, AppManager will display the same version number as **Help > About**.

Resource Object

Cisco CallManagers

Default Schedule

By default, this script runs **once** a week.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if discovery succeeds?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds.
SQL username (leave blank to use Windows authentication)	Provide the user login account required to access the CallManager SQL Server database. Leave this field blank to accept the default Cisco login account: `CiscoCCMCDR`. If you have changed the default password for `CiscoCCMCDR`, or want to use a different login account, configure the login and password using AppManager Security Manager before running this script. On the SQL tab of Security Manager, provide the IP address or hostname of the CallManager **SQL Server** computer, as well as the **SQL Login Name** and **SQL Login password**.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.

Parameter	How to Set It
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery returns some data but also generates warning messages. The default is 15.
Create cluster server group?	Set to **y** to arrange in a cluster all CallManagers in a server group. The cluster is visible in the Master view only. The default is y. By arranging your CallManagers in a cluster, you can simplify your monitoring process by running Knowledge Scripts on a cluster to monitor every CallManager in the cluster. The Discovery_CiscoCallMgr Knowledge Script groups CallManagers according to Publisher. A cluster consists of a Publisher and one or more Subscriber CallManagers. Only the Subscribers perform call processing. The Publisher handles administrative activities such as configuration. The following combinations represent the most common clusters: • **One Publisher and one Subscriber**. The Publisher server contains the TFTP server and any media resource applications. It also acts as the backup for the Subscriber. • **One Publisher and three Subscribers**. The Publisher server contains the TFTP server and any media resource applications. Two of the Subscribers are primary CallManagers. The remaining Subscriber is the backup for the two primaries. • **One Publisher, a TFTP server, and six Subscribers**. Either the Publisher or the TFTP server will contain the media resource applications. Four of the Subscribers are primary CallManagers. The remaining two are backups for the primaries. **Note** For the Discovery script, the default action on the **Actions** tab is Action_AddComputerToServerGroup. When creating a server group, do *not* change this default selection.

CiscoCM

Use the Discovery_CiscoCM Knowledge Script to discover resource and configuration information for Cisco Unified Communications Manager clusters. The Cisco AXL Web service, the Tomcat service, and the SOAP API services must be active on all servers in the cluster. Only one computer can act as proxy agent for any given Unified Communications Manager cluster. Therefore, run Discovery_CiscoCM on only one Windows server at a time

Prerequisites

Configure your AXL password in AppManager Security Manager before discovering Unified CallManager resources.

Use the Cisco Administration Web site to configure the proxy agent computer as a billing server. This configuration allows Unified CallManager to push call detail records (CDRs) to the proxy agent computer.

Configuring AXL Passwords

AVVID XML Layer (AXL), a Cisco application programming interface, enables Unified Communications Manager to access the HTTP server. Configure the AXL password in AppManager Security Manager *before* running the Discovery_CiscoCM Knowledge Script. Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`CiscoCM_AXL`
Sub-label	Indicates whether the AXL information will be used for a single Communications Manager or for all Communications Manager. • *For a single Communications Manager*, provide the name of the Communications Manager server. • *For all Communications Managers*, type `default`.
Value 1	AXL user ID that has the authority to use the AXL API. In most cases, the Communications Manager Administrator user has this authority.
Value 2	AXL password that has the authority to use the AXL API. In most cases, the Communications Manager Administrator user has this authority.
Value 3	Use this field *only* if you used Cisco Unified Communications Manager Administration to change the number of the HTTPS port the proxy agent computer uses to connect to the Communications Manager server. Type the new secure port number. Leave this field blank to use the default port number: 8443.
Extended application support	Required field. Encrypts the AXL password in Security Manager.

Configuring the Proxy Agent Computer as a Billing Server

To allow the Unified Communications Manager server to send Call Detail Records (CDRs) to the proxy agent computer, configure the Unified Communications Manager server to recognize the proxy agent computer as a billing application server.

Use the Cisco Unified Communications Manager Administration Web site to configure the proxy agent computer as a billing server.

Tip
If the proxy agent computer does not receive CDRs after you complete the following procedure, ensure the FTP server is working. Verifying FTP functionality usually eliminates most problems. If the FTP server is working as expected, then verify network connectivity. Firewalls can prevent the Unified Communications Manager server from sending CDRs to the proxy agent computer.

To configure the billing server:

1. Navigate to the Administration Web site of your primary Unified Communications Manager server.
2. In the **Navigation** field, select **Cisco Unified CallManager Serviceability** and then click **Go**.
3. In the Serviceability window, click **CDR Management** on the Tools menu.
4. In the CDR Management window, click **Add new** and complete the following fields:

Field	Description
Host Name/IP Address	DNS hostname or IP address of the proxy agent computer, which must be configured as an FTP or sFTP server.
User Name	User name required to access the proxy agent computer. If you use sFTP, provide the user name you used when configuring the sFTP server.
Password	Password required to access the proxy agent computer. If you use sFTP, provide the password you used when configuring the sFTP server.
Protocol	Indicates whether to use **FTP** or **sFTP** to push CDRs to the proxy agent computer.
Directory Path	Location to which CDRs are pushed on the proxy agent computer. Do not type a full path. Instead, type a relative path based on the FTP publishing folder on the proxy agent computer, which is, by default, `c:\inetpub\ftproot`. The path must include the TreeView cluster name and a trailing backslash (\). For example, if the TreeView cluster name is "CiscoCM:CCM80-01-Cluster," then type `CCM80-01\`. Files will be written to the following folder on the proxy agent computer: `c:\inetpub\ftproot\CCM80-01` **Important** If you are running Unified Communications Manager 5.x, use forward slashes (/), not backslashes (\), in your file path. In version 5.x, backslashes cause a corruption of the Cisco database. Backslashes are acceptable in later versions of Communications Manager.

Resource Object

Windows server

Only one computer can act as proxy for any given CallManager cluster. Therefore, run this script on only one computer at a time.

Default Schedule

By default, this script runs **once** a week.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_CiscoCM job fails. The default is 5.

Full path to file with list of primary CallManager servers	Specify the full path to a file on the proxy agent computer that contains a list of the DNS hostnames of the primary servers you want to monitor. The file should list the names on one or more lines. Separate multiple names in one line with a comma. For example,
	`primarycluster1,primarycluster2,primarycluster4`
	If you specify the names on multiple lines, ensure that each line contains only one entry. For example:
	`primarycluster1`
	`primarycluster2`
	`primarycluster4`
	Important
	• If DNS is not available in your environment, you can use IP addresses in this parameter.
	• After running the Discovery_CiscoCM job, note the name of the discovered cluster in the TreeView, which will look similar to the following example:
	`Proxy agent computer`
	`CiscoCM:`**`CCM80-01`**`-Cluster`
	• Even if you use IP addresses in this parameter, the text in bold, the *TreeView cluster name*, may look like a hostname.

Comma-separated list of primary CallManager servers	If you do not have a file that contains a list of server names or addresses, you can use this parameter to type the DNS hostnames of the primary servers in the clusters that you want to monitor. Separate multiple names with a comma. For example:
	`primarycluster1,primarycluster2,primarycluster4`
	Important
	• If DNS is not available in your environment, you can use IP addresses in this parameter.
	• After running the Discovery_CiscoCM job, note the name of the discovered cluster in the TreeView, which will look similar to the following example:
	`Proxy agent computer`
	`CiscoCM:`**`CCM80-01`**`-Cluster`
	• Even if you use IP addresses in this parameter, the text in bold, the *TreeView cluster name*, may look like a hostname.

Parameter	How to Set It

Comma-separated list of CallManager IP address pairs in a single NAT cluster	MSPs (Managed Service Providers) frequently maintain distributed customer networks in which NAT (Network Address Translation) is used to translate the IP address ranges that are monitored from a single NOC (Network Operations Center). The use of NAT prevents AppManager from recognizing the actual IP addresses of the servers in the remote cluster. If your AppManager agent is located on a server in the NOC, but the monitored devices are located in a cluster in the remote customer network, you need to provide a list of the IP addresses of the remote monitored devices.
	Use this parameter to enable AppManager to recognize the IP addresses of the servers for a single remote Communications Manager cluster.
	Type a list of IP address pairs for the Communications Manager servers in a remote cluster. Use commas to separate the addresses. A pair consists of a server's NAT (external) IP address and its IP address inside the cluster. The first address pair in the list must be that of the Communications Manager Publisher (also call the Primary Communications Manager), followed by address pairs for the Subscribers inside the remote cluster. Use the following format:
	`publisherexternaladdress,publisherinternaladdress,subscriberexternaladdress1,subscriberinternaladdress1,subscriberexternaladdress2,subscriberinternaladdress2`
	In the following example, the 10.41* addresses are externally visible and the 172.16* addresses are visible only to the Communications Manager servers:
	`10.41.1.10,172.16.1.10,10.41.1.11,172.16.1.11,...`

Raise event if discovery succeeds?	Select **Yes** to raise an event when discovery succeeds. The default is unselected.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25.
Raise event if discovery succeeds with warnings	Select **Yes** to raise an event if discovery returns some data but also generates warning messages. The default is Yes.
Event severity when discovery succeeds with warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discover generates warning messages. The default is 15.
Raise event if discovery fails?	Select **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery fails. The default is 5.
Discovery Details	
Display FQDN in TreeView for discovered servers?	Select **Yes** to display CiscoCM servers in the TreeView using fully qualified domain names (FQDNs) instead of the host name after you run discovery. Selecting this option does not affect the name of the top-level CiscoCM cluster object. The default is unselected.
Discover Trap Receiver?	Select **Yes** to discover NetIQ SNMP Trap Receiver. The default is Yes.
Trap Receiver IP address	Specify the IP address of the computer on which Trap Receiver is installed. The default is `localhost`.
Trap Receiver TCP port	Specify the TCP port number through which Trap Receiver will communicate with AppManager. The default is port 2735.

CiscoCM_4x

Use the Knowledge Script to discover a CallManager 4.x cluster. You can then use the CiscoCM_4x Knowledge Scripts to monitor phone deregistration on CallManager 4.x clusters.

Prerequisites

- The proxy agent computer must be running SQL Server or MSDE in order to provide a local database in which to store the collected deregistration information.
- Configure the AXL user ID and password in AppManager Security Manager before discovering a CallManager 4.x cluster. For more information, see CiscoCM_4x.

Resource Object

NT_MachineFolder

Only one computer can act as proxy for any given CallManager cluster. Therefore, run this script on only one computer at a time.

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_CiscoCM_4x job fails. The default is 5.

Full path to file with list of CallManager Publishers	Specify the full path to a file on the agent computer that contains a list of Publisher names or IP addresses. The file should contain the names or IP addresses on one or more lines. If you specify the names on one line, separate each item with a comma. For example,
	`10.0.1.1,10.0.1.254,10.0.4.1,10.0.4.254`
	If you specify the names on multiple lines, ensure that each line contains only one entry. For example:
	`primarycluster1`
	`primarycluster2`
	`primarycluster3`

Comma-separated list of CallManager Publishers	If you do not have a file that contains a list of Publisher names or IP addresses, you can use this parameter to type the names or IP addresses of the CallManager Publisher in the clusters that you want to monitor. For example: `primarycluster1,primarycluster2,primarycluster4`
Raise event if discovery succeeds?	Set to **Yes** to raise an event when discovery succeeds. The default is unchecked.

Parameter	How to Set It
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25.
Raise event if discovery succeeds with warnings?	Set to **Yes** to raise an event if discovery returns some data but also generates warning messages. The default is Yes.
Event severity when discovery succeeds with warnings	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discover generates warning messages. The default is 15.
Raise event if discovery fails?	Set to **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery fails. The default is 5.

CiscoCME

Use this Knowledge Script to discover Cisco CallManager Express (CME) resource and configuration information.

Prerequisites

Configure your AXL password and community string values in AppManager Security Manager.

AXL Password Configuration

AVVID XML Layer (AXL), a Cisco application programming interface (API), enables CallManager Express to access the CallManager Express HTTP server.

Most of the AXL information is configured in an IOS configuration mode called telephony-service. In order for the CiscoCME Knowledge Scripts to function properly, you should review and then take action on the following:

- `xmltest` cannot be configured on the CallManager Express router. This configuration keyword puts the AXL (AVVID XML Layer) into interactive test mode. If `xmltest` is configured, then the AXL queries that the CallManager Express Knowledge Scripts use will not work. Use the following IOS commands to disable `xmltest`:

  ```
  config t, telephony-service, no xmltest
  ```

- If the `xmlschema` keyword is configured on the CallManager Express router, then the CallManager Express Knowledge Scripts may not work properly. This configuration keyword specifies the location of the XML schema for AXL. By default, the Knowledge Scripts use the default schema location. If you change the keyword to something other than the default, then the Knowledge Scripts will not be able to identify the schema location.

If your AXL password information is the same for all CallManager Express devices, then complete the following procedure once. If your AXL password information is different for different devices, then complete the following procedure once for each different password.

Note
If, after running Discovery_CiscoCME, expected devices were not discovered, ensure you configured the correct AXL password. To do so, configure the AXL password again.

Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`CiscoCME`
Sub-label	Indicates whether the community string will be used for a single device or for all devices. • *For a single router*, provide the <*`device name`*>. • *For all routers*, type `default`.
Value 1	The AXL password that you configured using the `log password` IOS command on the router. If you did not configure an AXL password, enter the `Router privilege mode` password
Extended application support 3	Required field. Encrypts the AXL password in Security Manager.

SNMP Community String Configuration

To enable SNMP access of CallManager Express devices, configure the SNMP read-only community strings in AppManager Security Manager before discovering CallManager Express devices.

Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`NetworkDevice`
Sub-label	Indicates whether the community string will be used for a single device or for all devices. • *For a single device*, provide the <*`device IP address`*>. • *For all devices*, type `default`.
Value 1	The appropriate reade-only community string, such as `private` or `public`.
Value 3	Use this field *only* if you have used Cisco CallManager Administration to change the number of the HTTPS port the proxy agent computer uses to connect to the CallManager server. In the **Value 3** field, type the new secure port number. Leave this field blank to use the default port number: 8443.

Resource Object

You should only have one computer acting as a proxy for any given CallManager Express device. Therefore, drop this script on only one computer at a time.

Default Schedule

By default, this script is only run **once** for each server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Auto Discovery	
Default gateway router	Enter the IP network address of the gateway (router) to query during discovery. **Note** Use this parameter if you're not certain of all the relevant subnets that should be scanned during discovery. If you enter an IP address here, AppManager will query the gateway for its routing tables and then attempt to discover every device in the tables.
Maximum number of hops	Enter the maximum number of router hops that you want discover to make during auto-discovery. The default is one hop. Discovery considers the gateway router itself to be the first hop. Therefore, a **Maximum number of hops** setting of 1 means you'll only discover the networks directly connected to the gateway router, but no other routers. To discover more, enter a **Maximum number of hops** setting of at least 2.

Parameter	How to Set It
List of devices	Use this parameter if you know which CallManager Express devices you want to discover. Enter a list of the devices whose resources you want to discover. You must specify at least one device. Use commas to separate the names in the list: `raldbellijm02,raldattixlm`. You can enter hostnames (if you use DNS in your environment) or IP addresses. **Note** The AXL password and SNMP community string information for each of the devices that you list in this field must be entered into Security Manager before you can run this script.
List of device ranges	Enter a list of IP address ranges for the CallManager Express devices whose resources you want to discover. Spaces are invalid in the list; only numbers, dashes, periods, and commas are allowed. For example: `10.0.1.1-10.0.1.254,10.0.4.1-10.0.4.254`. **Note** Limit the number of IP addresses in each range to no more than 256. To scan more than 256 IP addresses, break a range into multiple ranges, each with no more than 256 IP addresses.
Full path to file with list of devices	Instead of listing each device separately (in the previous parameter), you can specify the full path to a file on the agent computer that contains a list of hostnames or IP addresses. The file should contain the names on one or more lines. If you specify the devices on one line, separate each item with a comma. For example: `10.0.1.1-10.0.1.254,10.0.4.1-10.0.4.254`. If you specify the devices on multiple lines, ensure that each line contains only one entry. For example: • `SEP999999994002` • `SEP999999994000` • `SEP999999994004` **Note** The AXL password and SNMP community string information for each of the network devices listed in the file must be entered into Security Manager before you can run this script.
Discovery Details	Use these parameters to limit discovery to certain types of devices, and to set a discovery timeout.
Discover individual …	This script automatically discovers interfaces, links, and ports when the following parameters are enabled (which is the default setting). **Note** To improve console performance, disable the following parameters for any of the devices that you are not interested in monitoring. By not displaying these objects in the TreeView pane, you will significantly speed up discovery and improve the performance of the TreeView pane of the Operator Console. … interfaces? … LAN links? … WAN links? … frame relay links? … ATM links? … FXS ports? … FXO ports? … ISDN channels?

Parameter	How to Set It
Discovery timeout	Enter the amount of time in minutes (no more than 60) that the script should attempt discovery before stopping and raising an unsuccessful discovery event. The default is 10 minutes.
Raise event when discovery succeeds?	This script always raises an event when discovery fails for any reason. In addition, you can enable this parameter to raise an event when discovery succeeds. The default is n.
Event severity when discovery …	Set the event severity level, from 1 to 40, to reflect the importance when the job: • ... **succeeds**. If you set this script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25. • ... **fails**. The default is 5.

CiscoCNS_PerfE

Use this Knowledge Script to discover Cisco CNS Performance Engine (CNS-PerfE) resource and configuration information.

Prerequisite

Configure Security Manager with the password that is required for accessing the CNS-PerfE computer.

Note
The password to access the CNS-PerfE computer is the password used for the CNS bus (such as when sending the TIBCO messages to the CNS-PerfE). The default password is cisco. You can change this password using the Settings page of the CNS-PerfE Web Interface. For more information, refer to your CNS Performance Engine User Guide.

You *cannot* discover the Cisco CNS-PerfE managed object until you configure the password in Security Manager.

To configure the CNS-PerfE password:

1. From the Operator Console, click **Extensions > Security Manager**.
2. Expand the Computers branch and select the computer on which the Cisco CNS-PerfE managed object is installed.
3. Click the **Custom** tab.
4. Click **Add**. The Add Custom Entry dialog box is displayed.
5. In the **Label** field, enter `CNSPE`.
6. In the **Sub-label** field, enter `<hostname of Solaris machine>` or `default`.
7. In the **Value 1** field, enter `<CNS-PerfE password>`.
8. In the **Value 2** field, enter <ftp password>.
9. Click **Apply**.

Resource Objects

NT_MachineFolder

Default Schedule

By default, this script runs **once** for each server.

Setting Script Parameters

Set the following parameters as needed:

Parameter	How to Set It
Hostname or IP address	Enter the hostname or IP address of the Solaris or Linux computer where the Cisco CNS-PerfE is located. The information you enter here will appear in the TreeView pane to identify the Cisco CNS-PerfE computer. **Note** Be sure to enter the information correctly. The Solaris or LINUX machine requires case sensitivity.
CNS-PerfE subject	Enter the TIBCO subject field information for which the Cisco CNS-PerfE is listening. Leave this parameter blank if you want to use the default: `cisco.mgmt.das.<CNS-PEhostname>`. **Notes** • You can confirm the subject field information by checking the CNS name shown on the CNS-PerfE Web interface home page. • If you configured a dotted-decimal IP address in the previous parameter, then you must specify the subject. You cannot leave this parameter blank.
Create default schedules?	Set to **y** to create default schedules that match the schedule defaults in the CiscoCNS Knowledge Scripts. If set to **y**, a Schedules folder will appear below the Cisco CNS-PerfE object in the TreeView pane.
Raise event if discovery succeeds?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • ... **succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • ... **fails**. The default is 5 (red event indicator).

CiscoICD

Use this Knowledge Script to discover a computer where the Cisco ICD (Integrated Contact Distribution) managed object is installed. With successful discovery, the Cisco ICD object is created in the TreeView pane.

Resource Object

CiscoICD server

Default Schedule

By default, this script runs **once** every week.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if discovery succeeds?	Set the event severity level, from 1 to 40, to indicate the importance of the event when discovery succeeds. The default is 25 (blue event indicator).
Event severity when discovery succeeds	Set the severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Raise event if discovery fails?	Select the **Yes** check box to raise an event when discovery fails. By default, events are enabled.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of the event when discovery fails. The default is 5.
Raise event if discovery partially succeeds?	Select the **Yes** check box to raise an event when discovery returns some data but also generates warning messages. By default, events are enabled.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event when discovery partially succeeds, returning some information but also generating a warning message. The default is 15 (yellow event indicator).
Discovery	Use this parameter to specify the type of security authentication to use.
SQL username	If appropriate, enter your SQL username. Leave this field blank to use Windows Authentication. The default is blank. **Note** If a SQL username is required, then you must configure the username in the AppManager Security Manager. For more information, see the *Installation Guide* for AppManager.

CiscoICM

Use this script to discover the Cisco ICM configuration and resources.

Prerequisite

Discover Windows resources on the server that you want to monitor *before* you discover ICM resources. If you have not yet discovered Windows resources, run the NT discovery script.

Resource Objects

Cisco ICM servers

Default Schedule

By default, this script is **run weekly** for each server.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if discovery succeeds? (y/n)	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery returns some data but also generates warning messages. The default is 15.
SQL User Name (leave blank to use Windows authentication)	If appropriate, provide your SQL user name. Leave this field blank to use Windows Authentication. Ensure the user has permission to access the database in read-only mode. If you want to use a specific SQL Server login account, use Security Manager to update the AppManager repository with the SQL Server login you want to use. For more information, see the *Installation Guide for AppManager*.
Central controller database detection	Select whether you want AppManager to automatically identify the Central Controller database or whether you want to enter the database name manually. AppManager can only detect the Central Controller database automatically if you installed the Central Controller on the Admin Workstation computer. The default is Automatic.
Name of server hosting central controller database	Enter the computer where the Central Controller database. You can enter a host name, IP address, or fully qualified domain name.
Name of central controller database	Enter the name of the Central Controller database.

CiscoICS

Use this Knowledge Script to discover Cisco ICS configuration and resources.

Prerequisite

Discover Windows resources on the server that you want to monitor *before* you discover ICS resources. If you have not yet discovered Windows resources, run the NT discovery script.

Resource Objects

Cisco ICS servers

Default Schedule

By default, this script is only run **once** for each server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when discovery succeeds?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • ...**succeeds**. If you enabled events when the job succeeds, set the event severity level for a successful discovery. • ...**fails**. The default is 5 (red event indicator). • ...**partially succeeds**. Set the event severity level for a discovery job that returns some data but also generates warning messages.

CiscoIPTSecurity

Use this Knowledge Script to discover security-related applications, such as Cisco Security Agent (CSA) and Symantec AntiVirus, on the Cisco IP telephony servers on which you installed the Cisco IP Telephony Security module.

Resource Object

NT_MachineFolder

Default Schedule

By default, this script runs **weekly on Sunday**.

Setting Script Parameters

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the discovery job fails. The default is 5.
Raise event if discovery succeeds?	Set to **Yes** to raise an event when discovery completes successfully. The default is unchecked.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery completes successfully. The default is 25.
Raise event if discovery fails?	Set to **Yes** to raise an event when discovery fails to complete. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery fails to complete. The default is 5.

CiscoIPTV

Use this Knowledge Script to discover the Cisco IP/TV resources and configuration on computers where the Cisco IP/TV managed object is already installed.

Prerequisite

Discover Windows resources on the server that you want to monitor *before* you discover IP/TV resources. If you have not yet discovered Windows resources, run the NT discovery script.

Resource Objects

Cisco IP/TV servers.

Default Schedule

By default, this script is only run **once** for each server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if discovery succeeds?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: ...**succeeds**. If you enabled events when the job succeeds, set the event severity level for a successful discovery. ...**fails**. The default is 5 (red event indicator). ...**partially succeeds**. Set the event severity level for a discovery that returns some data but also generates warning messages.

CiscoIVR

Use this Knowledge Script to discover Cisco IVR resources and configuration.

Prerequisite

Discover Windows resources on the server that you want to monitor *before* you discover IVR resources. If you have not yet discovered Windows resources, run the NT discovery script.

Resource Objects

Cisco IVR servers.

Default Schedule

By default, this script is run **weekly for each server**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if discovery succeeds?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery that returns some data but also generates warning messages.

CiscoPersonalAsst

Use this Knowledge Script to discover the Cisco Personal Assistant configuration and resources.

Prerequisite

Discover Windows resources on the server that you want to monitor *before* you discover Personal Assistant resources. If you have not yet discovered Windows resources, run the NT discovery script.

Resource Objects

Cisco Personal Assistant servers

Default Schedule

By default, this script is only run **once** for each server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if discovery succeeds?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery that returns some data but also generates warning messages.

CiscoUE

Use this Knowledge Script to discover Cisco Unity Express resources and configuration information.

AppManager uses SNMP queries to remotely access Unity Express devices. However, it cannot communicate with the devices unless it has permission to do so. You can grant that permission by configuring the appropriate SNMP community string information into AppManager Security Manager.

Prerequisite

AppManager uses SNMP queries to remotely access Unity Express devices. However, it cannot communicate with the devices unless it has permission to do so. You can grant that permission by configuring the appropriate community string information into AppManager Security Manager.

For each Unity Express device that you want to monitor, the SNMP community string information *must* be entered into Security Manager before you can discover Unity Express resources.

In some cases, Unity Express can re-use the default community string that you may have already configured for the AppManager for Network Device module. Use the following table to determine which community string information you should enter:

If	And	Then
You have configured the community string for Network Device	The community string is the same for Unity Express	Do *not* re-enter the community string. AppManager can use the community string settings for Network Device.
You have *not* configured the community string for Network Device	The community string is the same for Unity Express	Use the following procedure to enter the community string for Network Device. AppManager can use the community string settings for Network Device.
You have *not* configured the community string for Network Device	The community string is *not* the same for Unity Express	Use the following procedure to enter the community strings for *both* Unity Express *and* Network Device.

In summary, you always need the community string information for AppManager for Network Device. If the community strings are different for the two modules, then you also need the community string information for Unity Express.

Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`CiscoUE` or `NetworkDevice`, as appropriate
Sub-label	For a single device on a particular proxy: • *For Cisco UE*, enter the <*`device IP address`*> • *For Network Device*, enter the <*`hostname or device IP address`*> For all devices on a particilar proxy, enter `default`.
Value 1	The appropriate read-only community string, such as `public` or `private`.
Value 2	AXL password that has the authority to use the AXL API. In most cases, the CallManager Administrator user has this authority.

Resource Object

Cisco Unity Express routers

Default Schedule

Discovery runs **every Sunday at 3 A.M.**, but also runs immediately on the first iteration of the job.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the discovery job fails. The default is 5.
Raise event if discovery succeeds?	Set to **Yes** to raise an event when the discovery process is successful. The default is unchecked.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25.
Raise event if discovery fails?	Set to **Yes** to raise an event when the discovery process fails to find some or all of your Unity Express resources. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery fails to find some or all of your Unity Express resources. The default is 10.
Discovery Details	
Discover individual ... ?	Set any of the Discovery Details parameters to **Yes** to discover the following components: • Interfaces • LAN links • WAN links • Frame relay links • ATM links • FXS ports • FXO ports • ISDN channels
Auto Discovery	
Default gateway router	Enter the IP network address of the gateway router to query during discovery. The router you want to query is the router that hosts the Unity Express device that you want to monitor. **Note** Use this parameter if you're not certain of all the relevant subnets that should be scanned during discovery. If you enter an IP address here, AppManager will query the gateway for its routing tables and then attempt to discover every device in the tables.
Maximum number of hops	Enter the maximum number of hops that you want discovery to make during auto-discovery. The default is one hop. Discovery considers the gateway router itself to be the first hop. Therefore, a **Maximum number of hops** setting of 1 means you'll only discover the networks directly connected to the gateway router, but no other routers. To discover more, enter a **Maximum number of hops** setting of at least 2.
Discover Unity Express Devices	

Parameter	How to Set It
Discovery timeout	Enter the number of minutes (no more than 60) that the script should attempt discovery before stopping as an unsuccessful discovery. The default is 10 minutes.
Maximum number of concurrent discoveries	Specify the maximum number of Unity Express devices that can be queried for discovery at one time. No matter what value you enter, discovery is still performed for the entire list of devices that you specify in the following parameters. Setting this parameter to a low value throttles the number of SNMP requests performed at one time, but may increase the overall time it takes to discover a list of devices. The default is 10 concurrent discoveries.
List of IP telephony routers	Use this parameter if you know which IP telephony routers you want to discover, which are those routers that host Unity Express devices. Specify at least one router IP address or hostname, using a comma to separate multiple items: `10.0.1.1,10.0.1.7` You can enter IP addresses or hostnames, but you *must* enter the same IP address or hostname for which you configured SNMP community string information. If you configured a community string for a hostname, then enter the *same* hostname; if you configured an IP address, then enter the *same* IP address.
List of IP telephony router ranges	Enter a list of IP address ranges of the routers for which you want to discover resources. Spaces are invalid in the list; only numbers, dashes, periods, and commas are allowed. For example: `10.0.1.1-10.0.1.254,10.0.4.1-10.0.4.254` The routers you specify are those routers that host Unity Express devices. Their IP addresses *must* match the IP addresses for which you configured SNMP community string information. If you configured community strings for hostnames, then don't use this parameter. Use the following parameter or the preceding parameter. **Note** Limit the number of IP addresses in each range to no more than 256. To scan more than 256 IP addresses, break a range into multiple ranges, each with no more than 256 IP addresses.
Full path to file with list of IP telephony routers	Instead of listing each router separately, you can specify the full path to a file on the agent computer that contains a list of IP addresses or hostnames of routers that host Unity Express devices. The list should contain the names/addresses on one or more lines. If you specify the routers on one line, separate each item with a comma. For example: `10.0.1.1-10.0.1.254,10.0.4.1-10.0.4.254` If you specify the routers on multiple lines, ensure that each line contains only one entry. For example: • `routername01` • `routername02` • `routername10` You can enter IP addresses or hostnames, but you *must* enter the same IP address or hostname for which you configured SNMP community string information. If you configured a community string for a hostname, then enter the *same* hostname in the list; if you configured an IP address, then enter the *same* IP address in your list.

Parameter	How to Set It
Comma-separated list of Unity Express and host router NAT-enabled IP address pairs	MSPs (Managed Service Providers) frequently maintain distributed customer networks in which NAT (Network Address Translation) is used to translate the IP address ranges that are monitored from a single NOC (Network Operations Center). The use of NAT prevents AppManager from recognizing the actual IP addresses of the remote Unity Express devices and host routers. If your AppManager agent is located on a server in the NOC, but the monitored devices are located in the remote customer network, you need to provide AppManager with a list of the IP addresses of the remote monitored devices. Use this parameter to enable AppManager to recognize the IP addresses of the remote Unity Express devices and host routers. Type a list of IP address pairs for the remote Unity Express devices and host routers. Use commas to separate the addresses. A pair consists of the externally visible IP address for a Unity Express device and the externally visible IP address of its host router. Use the following format: `UEexternaladdress1,hostrouterexternaladdress1,UEexteraladdress2,hostrouterexternaladdress2` The following example shows how the pairs look when you use IP addresses: 10.41.1.10,10.41.1.11,10.41.1.12,10.41.1.13

CiscoUnity

Use this Knowledge Script to discover Cisco Unity resources (including the TSP version) and ports.

Prerequisite

Discover Windows resources on the server that you want to monitor *before* you discover Unity resources. If you have not yet discovered Windows resources, run the NT Discovery Knowledge Script.

Resource Objects

Cisco Unity servers

Default Schedule

By default, this script is run **weekly** for each server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if discovery succeeds?	This script always raises an event when the discovery fails for any reason. In addition, you can set this parameter to y to raise an event when the job succeeds.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery that returns some data but also generates warning messages.
SQL username (leave blank to use Windows authentication)	If appropriate, enter your SQL username. Leave this field blank to use Windows Authentication. If you want to use a specific SQL Server login account, use Security Manager to update the AppManager repository with the SQL Server logins you want to use. For more information, see the *Installation Guide* for AppManager.
Create failover pair server group (in Master view)?	Set to **y** to create a server group composed of a failover pair (primary and secondary Unity servers). This server group is visible in the TreeView pane from the Master view only.

CiscoUnityBridge

Use this Knowledge Script to discover Cisco Unity Bridge configuration and resources. This script automatically raises an event when discovery is unsuccessful.

Prerequisite

Discover Windows resources on the server that you want to monitor *before* you discover Unity Bridge resources. If you have not yet discovered Windows resources, run the NT discovery script.

Resource Objects

Cisco Unity Bridge servers

Default Schedule

By default, this script is run **once** for each server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to y to raise an event when the job succeeds.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery that returns some data but also generates warning messages.

Cluster

Use this Knowledge Script to discover clustered applications on physical and virtual machines. This script also discovers a virtual server cluster alias and adds it as a top-level object in the TreeView.

This script facilitates monitoring of clustered applications. It removes the need to run the SetResourceDependency Knowledge Script or run multiple jobs on each clustered node per instance of the application. Also, application failovers are not required to discover servers on each node.

Though virtual servers are viewed and monitored as objects in the TreeView, features like pinging the physical computer are not available. Other settings like maintenance mode, custom server properties and security information storage are not applicable for virtual machines.

Security Rights. To correctly discover and monitor a Microsoft cluster, this Knowledge Script requires local Administrator access to each node of the Microsoft cluster. To do this, run the `netiq` service as a domain user account and a member of the local Administrator group on each member of the cluster. Without this access, the discovery fails because it relies on the Microsoft Cluster API to properly access cluster resources.

Administering a Cluster. The Cluster Administrator can be used to administer a cluster, provided the account you are using has the required permissions and group memberships. The local Administrator account and local system account always have access to the cluster. You can use another account to administer a cluster with Cluster Administrator provided that this account:

- has permission to administer the cluster. You must use Cluster Administrator to assign permissions, not Windows Group Administrator.
- is a domain account, which is a member of the local Administrators group.
- is a member of the local Administrators group on each node of the cluster.

The account can be a member of other groups, such as global groups, as long as it is a domain account.

By default, this Knowledge Script raises an event when discovery fails.

Note
This Knowledge Script is not supported on AppManager version 6.x.

Prerequisite

Use the NT Knowledge Script to discover Microsoft Windows resources on the server you want to monitor before you discover clustered applications.

Resource Objects

Microsoft Clustered Servers

Default Schedule

By default, this script is run **once** for each server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when discovery succeeds?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the Discovery_Cluster job succeeds.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery returns some data but also generates warning messages. The default is 10.
Event severity when discovery is not applicable	Set the event severity level, from 1 to 40, to reflect the importance of an event when discovery is not applicable. The default is 15.

Dell

Use this Knowledge Script to discover Dell server configuration and resources. This Knowledge Script requires SNMP and the Dell OpenManage agent (Hardware Instrumentation Program or HIP) to be running on the computer you are discovering. If a required service is not found or is not running, the Discovery job fails with a "Not a Dell server" event.

Resource Object

Dell servers

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to y to raise an event when the job succeeds. The default is n.
SNMP community string	Provide the SNMP community string required to access AdapterSCSI resources. Provide the same community screen you entered into AppManager Security Manager. If you did not configure community string information in Security Manager, then provide the default community string of `public`.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have a Dell Server installed. The default is 15 (yellow event indicator). **Note** If required services, such as SNMP or Dell OpenManage HIP, aren't running on the computer you are discovering, you may see a severity 15 event (Not a Dell server). If you see this type of event, see the detail message for more information about what caused the discovery to fail.

Domino

Use this Knowledge Script to discover the configuration and databases associated with Lotus Domino Servers, including partitioned servers.

Resource Objects

Lotus Domino servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Discovery Targets	
Database discovery level	Because a server can have hundreds of Domino databases, this parameter is used to control which databases are discovered. Select a level to determine which databases are discovered: • **Root**=Notes data directory databases and mailboxes. • **+Mail**=root functionality + root\mail databases and all mailboxes below root. • **All**=all databases and mailboxes root and below. • **User**=only the databases specified in the database list. The default is All.
Database names, including `.nsf` (when level=User)	If the database discovery level is set to **User**, enter the names of the specific databases you want to discover, separated by commas with no spaces. Each database name should be relative to the Notes data directory. For example: `MyData.nsf,mail\mymail.box`
Save the discovery results file?	Select **Yes** to save the discovery results file. The default is Yes.
Save as...	Enter the full path to the discovery results file. For example: <HKLM\SOFTWARE\NetIQ\AppManager\4.0\InstallPath>\Discovery_<SERVER>.txt
Event Notification	
Raise event when discovery succeeds?	Select **Yes** to raise an event when the job succeeds. The default is unselected.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue event indicator).
Raise event when discovery fails?	Select **Yes** to raise an event when the Discovery_Domino job fails to discover Lotus Domino resources. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_Domino job fails to discover Lotus Domino resources. The default is 5 (red event indicator).

Parameter	How to Set It
Raise event when discovery partially succeeds?	Select **Yes** to raise an event when discovery returns some data but also generates warning messages. The default is Yes.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery returns some data but also generates warning messages. The default is 10 (red event indicator).
Raise event when discovery not appropriate?	Select **Yes** to raise an event when discovery is not appropriate. This type of failure usually occurs when the target computer does not have Lotus Domino Server installed or does not have the AppManager for Lotus Domino module installed.
Event severity when discovery not appropriate	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery is not applicable. The default is 15 (yellow event indicator).

Domino-RT

Use this Knowledge Script to discover if AppManager ResponseTime for Domino components are available on a specific managed client. At the Operator Console, drag this Knowledge Script to the managed client on which you are performing discovery.

After successful discovery, a new thumbnail appears in the TreeView pane with a list of machines that support it. Also, a new Domino-RT Knowledge Script pane will appear.

Resource Objects

Windows XP Professional, Windows 2000, or Windows NT

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery? [y/n]	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when Discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. This type of failure usually occurs when the target computer does not have all the prerequisites installed. The default is 10 (red event indicator).

Exchange

Use this Knowledge Script to discover Microsoft Exchange Server 5.5 (or earlier) and Microsoft Exchange 2000/2003 configuration and resources.

In Exchange 2003 it is possible to change the location of the Exchange tracking logs through the Exchange System Manager. If you do that, you must rediscover the new log path, so always re-run discovery after changing the location of an Exchange tracking log.

Note
To discover and monitor Exchange 2000 Server or Exchange Server 2003, you must delegate Exchange View Only Administrator permission to the monitoring service Log On As account. The AppManager setup program does not delegate permission to the monitoring service Log On As account.

Resource Objects

Exchange Server 5.5 (or earlier), Exchange 2000 Server, Exchange Server 2003.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to y to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have Exchange Server installed. The default is 15 (yellow event indicator).

Exchange2007

Use this Knowledge Script to discover configuration and resources for Microsoft Exchange Server 2007 and 2010 in both clustered and non-clustered environments.

Note
If you delete a resource object or add a resource object, such as a Mailbox or Public Folder database, you will need to run the Discovery_Exchange2007 script again to update the remaining objects. This behavior occurs on DAG and Standalone Mailbox roles.

Resource Objects

- NT_MachineFolder
- NT_VIR_MachineFolder

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Specify the severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_Exchange2007 job fails. The default is 5.
Discovery	
Event Notification	
Raise event if discovery succeeds?	Select **Yes** to raise an event if discovery succeeds. The default is unselected.
Event severity when discovery succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25.
Raise event if discovery fails?	Select **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when discovery fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery fails. The default is 5.
Raise event if discovery partially succeeds?	Select **Yes** to raise an event if discovery returns some data but also generates warning messages. The default is Yes.
Event severity when discovery partially succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery returns some data but also generates warning messages. The default is 10.

ExchangeDAG

Use this Knowledge Script to discover configuration and resources for a Microsoft Exchange Server 2010 Database Availability Group (DAG). Run Discovery_ExchangeDAG on an Exchange Server 2010 server to discover the virtual object for DAG. After you discover the virtual object, you must run the Exchange2007 Discovery Knowledge Script on the newly discovered object so you can discover the databases.

Resource Objects

- NT_MachineFolder
- NT_VIR_MachineFolder

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Specify the severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_ExchangeDAG job fails. The default is 5.
Discovery	
Event Notification	
Raise event if DAG discovery succeeds?	Select **Yes** to raise an event if DAG discovery succeeds. The default is unselected.
Event severity when DAG discovery succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which DAG discovery succeeds. The default is 25.
Raise event if DAG discovery fails?	Select **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when DAG discovery fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery fails. The default is 5.

Exchange-RT

Use this Knowledge Script to discover if AppManager ResponseTime for Exchange components are available on a specific managed client. At the Operator Console, drag this Knowledge Script to the managed client on which you are performing discovery.

After successful discovery, a new thumbnail appears in the TreeView pane with a list of machines that support it. Also, a new Exchange-RT Knowledge Script pane will appear.

Resource Objects

Windows Server 2008, R2; Windows Server 2008 (32-bit or 64-bit), Windows Server 2003 (32-bit or 64-bit), Windows XP, or Windows 2000

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can select the **Yes** check box to raise an event when the job succeeds. By default, events are not raised on success.
Event severity when Discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. This type of failure usually occurs when the target computer does not have all the prerequisites installed. The default is 10 (red event indicator).

HIS

Use this Knowledge Script to discover Microsoft Host Integration Server configuration and resources.

Although discovery of **primary** servers is successful when the NetIQ AppManager Client Resource Monitor is configured to run using a local system account, discovery of **backup** servers will only be successful when the NetIQ AppManager Client Resource Monitor is configured to use an account that is part of the local administrator's group.

Resource Object

Host Integration Server

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity level when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...partially succeeds**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have Microsoft Host Integration Server installed or does not have the AppManager managed object for Host Integration Server. The default is 15 (yellow event indicator).

HPNS

Use this Knowledge Script to discover Hewlett-Packard NetServer configuration and resources. This Knowledge Script requires SNMP and the HPNS support program to be running on the computer you are discovering. If a required service isn't found or isn't running, the Discovery job fails with a "Not an HPNS server" event.

Resource Object

HP NetServer servers

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
SNMP community string	Enter the SNMP community name to use. The default is the community name entered in the AppManager Security Manager or public if no community name has been entered.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have HPNS installed. The default is 15 (yellow event indicator). **Note** If required services, such as SNMP or HPNS, aren't running on the computer you are discovering, you may see a severity 15 event (Not a HPNS server). If you see this type of event, see the detail message for more information about what caused the discovery to fail.

IIS

Use this Knowledge Script to discover Microsoft Internet Information Server (IIS) configurations and resources.

This Knowledge Script looks for the IIS managed object to make sure the necessary software has been installed to enable monitoring. Managed objects, DLLs or executables, provide resources to help the Knowledge Scripts perform jobs. Each Knowledge Script processes information from the managed object and sends that information to the managed client. The managed client generates event and data information and sends the information to the management server.

Note
This Knowledge Script cannot discover IIS sites whose names are longer than 128 characters.

Resource Objects

IIS servers

Default Schedule

By default, this script is only run once for each computer.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. Default is n.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance when discovery is successful. The default is 21.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance when discovery fails. Discovery can fail if it finds no IIS instances, or no instances of the AppManager for IIS managed object. It also fails if it can find both IIS instances and the managed object, but there is nothing to discover (in the case that all services and sites have been deleted). Default is 5.

ISA

Use this Knowledge Script to discover Microsoft Internet Security and Acceleration (ISA) Server 2000 configurations and resources.

Resource Objects

ISA servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have ISA Server installed. The default is 15 (yellow event indicator).

MFXP

Use this Knowledge Script to discover Citrix XenApp or Presentation Server resources and configuration information. The TreeView for this module now includes a reorganized set of objects that include Citrix XenApp or Presentation Server, License Servers, Licenses, Farms, and Servers, along with two additional Services: MFCom and CitrixLicensing.

AppManager for Citrix MetaFrame supports cluster discovery on all cluster nodes for the Citrix License Server component. If you run the Discovery Knowledge Script on both nodes of a cluster added to the Operator Console, the Discovery script only discovers the license server on the active node. The TreeView for cluster discovery displays the license types available on the License Server object for all active cluster nodes only.

Resource Objects

Windows machine objects

Default Schedule

By default, this script is only run **once** for each server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when discovery succeeds?	Select **Yes** to raise an event if the discovery process is successful. The default is unselected.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the discovery process is successful. The default is 21.
Event severity level when discovery partially succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a discovery returns some data but also generates warning messages. The default is 11.

ModuleBuilder

Use this Knowledge Script to discover all known components for your Module Builder application on your selected computer. When AppManager discovers a component for your application, that component displays as a discovered resource for management in AppManager.

Resource Object

Module Builder application

Default Schedule

The default setting for this script is to run once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Discovery Failure	
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the discovery job fails. The default is 5.
Partial Discovery	
Allow partial discovery?	Select **Yes** to allow a partial discovery, in which some objects were discovered successfully, but others could not be discovered.The event details for a partial discovery lists the items that were not discovered. The default is Yes.
Event severity when discovery partially succeeds	If you set this Knowledge Script to allow a partial discovery, set the event severity level for a partial discovery. The default is 15.
Successful Discovery	
Raise event if discovery fully succeeds?	Select **Yes** to raise an event when the discovery process fully succeeds, without any warnings. The default is unselected.
Event severity when discovery fully succeeds	If you set this Knowledge Script to raise an event when the job fails, set the event severity level for a failed discovery. The default is 25.
Log File	**Note** This section lists any log files selected in the Log Files component of the Module Builder Editor. If you did not define log files for monitoring, this section will not appear in the Discovery Knowledge Script parameters.
[Log File Name]	The name of each log file selected in the ModuleBuilder Editor is listed in this section, with the following two parameters associated with that log file.
Create log file object if file is not present	In the ModuleBuilder Editor, the subject matter expert or the AppManager expert can set up conditions for a log file that currently does not exist. Select **Yes** to create the log file object even if the log file is not found during discovery. Unselect this option if you do not want to create the log file object if the log file is not found. If the discovery process does not find a specified log file, a partial discovery notification is created. The default is Yes.
Log file path	Specify a new path for the location of the log file, as needed. You should modify this log file path on agent computers where the log file might be located in a different directory.

MOMReportAgent

Use this Knowledge Script to discover the AppManager Report Agent for MOM that is installed by the XMP Modules Report Module Setup program.

Raising an event when discovery of the Report Agent succeeds is optional. Events are always raised when discovery fails, or when there is partial discovery. Partial discovery occurs if a MOM database has not been updated with the stored procedures used by the Report Agent.

Resource Objects

Any Windows computer where you have installed an AppManager Report Agent for MOM.

Default Schedule

The default schedule is Run **once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	Set to **y** to raise events. The default is n.
Severity level when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).
Severity level for partial discovery	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10 (red level indicator).

MQSeries

Use this Knowledge Script to discover IBM MQSeries queues, queue managers, channels, and servers.

Resource Objects

MQSeries servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have MQSeries installed. The default is 15 (yellow event indicator).

MSCS

Use this Knowledge Script to discover Microsoft Cluster Server (MSCS) configuration and resources. You can run this Knowledge Script on any node in the cluster.

Note
You should only add and discover actual cluster nodes. You should not attempt to add or discover virtual servers.

Resource Objects

MSCS servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have MSCS installed. The default is 15 (yellow event indicator).

Example of How this Knowledge Script Is Used

If you discover multiple nodes that are part of the same cluster, you may see what appear to be duplicate entries in the application view. For example, assume you have a SQL Server cluster with the computers `LOBO1` and `LOBO2`. Both of these computers are displayed in the Master view. After you run the SQL discovery to discover the cluster, `LOBO1` and `LOBO2` display the resource object `SQL Server:LOSLOBOS_SQL` in the Master view. `LOSLOBOS_SQL` represents the virtual server.

When you discover clustered applications such as Exchange and SQL Server, the discovered objects use the virtual server name (for example, LOSLOBOS_SQL). When you run the MSCS discovery, the discovered objects use the physical node name. For example, using the physical nodes and virtual server names described in this example, after running Discovery_MSCS, the Master view should display `MSCS Server:LOBO1` under `LOBO1`, and `MSCS Server:LOBO2` under `LOBO2`.

MSMQ

Use this Knowledge Script to discover Microsoft Message Queue Server (MSMQ) configuration and resources.

Discovery of private queues on a server that only contains private queues will only be successful when the NetIQ Client Resource Monitor is configured to use an account that is part of the local administrator's group.

Resource Objects

MSMQ servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
User name for SQL Server	Enter the username for logging on to the MSMQ SQL Server. The username must have permission to access SQL Server on the target machine(s). The default is the sa user account.
Use password from AppManager Security Manager	Set to **y** to use the SQL Server password you have entered into the AppManager repository with the AppManager Security Manager. The default is y.
Password for SQL Server	Enter the password for the SQL Server user name if you aren't using a password you have stored into the AppManager repository with the AppManager Security Manager. If you are using the password entered in the Security Manager, leave this field blank.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 30 (blue event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have MSMQ installed. The default is 15 (yellow event indicator).

MTS

Use this Knowledge Script to discover Microsoft Transaction Server (MTS) configuration and resources.

Resource Objects

MTS servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have MTS installed. The default is 15 (yellow event indicator).

NetAppFiler

Discovers a list of Network Appliance filers you want to remotely manage from a proxy server. To discover Network Appliance filer resources, run this Knowledge Script on a proxy server and specify the list of filers you want.

To discover a filer, security information about the filer must be specified on the proxy server using AppManager Security Manager.

Resource Objects

Windows computer acting as the Network Appliance filer proxy server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event if the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
List of filers to discover	A comma-separated list of Network Appliance filer names. If a Network Appliance filer name cannot be resolved, you can use an IP address.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...partially succeeds**. This Knowledge Script raises an event when only some filers in the list are discovered, and others are not. The default is 10 (red event indicator). • **...fails**. The default is 5 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have a Network Appliance filer installed. The default is 15 (yellow event indicator).

NetBackup

Use this Knowledge Script to discover Symantec NetBackup server resources and configuration information on Microsoft Windows computers.

Resource Objects

NetBackup servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator).

NetBackupUNIX

Use this Knowledge Script to discover Symantec NetBackup resource and configuration information on UNIX servers.

Resource Objects

UNIX servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise events when discovery succeeds? (y/n)	Select **y** to raise an event if the discovery job succeeds. This Knowledge Script raises an event even if the job fails for any reason. The default is n.
Search path for NetBackup programs	Type the path to the NetBackup program to direct the search for NetBackup resources. The default is `/usr/openv` (the default NetBackup installation path).
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. Set the severity level for a successful discovery and to raise an event when the job succeeds. The default is 25. • **...fails**. The default is 5. • **...partially succeeds**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 15. • **...is not applicable**. This type of failure usually occurs when NetBackup is not installed on the target computer. The default is 15.

Netfinity

Use this Knowledge Script to discover the resource and configuration information for IBM Netfinity Servers running Netfinity Manager. This Knowledge Script requires SNMP to be running on the computer you are discovering. If a required service is not found or is not running, the Discovery job fails with a "Not an Netfinity server" event.

Because SNMP is not installed on IBM Netfinity Servers by default, you may need to install it and restart the server before you can run this Knowledge Script successfully.

Resource Objects

Netfinity Manager servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
SNMP community string	Enter the SNMP community name to use. The default is the community name entered in the AppManager Security Manager or public if no community name has been entered.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have Netfinity Manager installed. The default is 15 (yellow event indicator). **Note** If required services, such as SNMP, aren't running on the computer you are discovering, you may see a severity 15 event (Not a Netfinity server). If you see this type of event, see the detail message for more information about what caused the discovery to fail.

NetfinityDir

Use this Knowledge Script to discover the resource and configuration information of IBM Systems Director.

When the discovery process completes successfully, IBM Systems Director Knowledge Scripts appear in the **Netfinity** view of the Operator Console in the NetfinityDir tab of the Knowledge Script pane.

Resource Objects

IBM Systems Director servers

Default Schedule

By default, this script is only run **once** for each computer. To ensure the best performance of this Knowledge Script, NetIQ Corporation recommends that you do not run this script more than once an hour.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to y to raise an event when the job succeeds. The default is n.
SNMP community string	Provide the SNMP community name of the IBM Systems Director server. The default is either the community name entered in AppManager Security Manager or *public* if no community name has been entered.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25. • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 15. • **...fails**. The default is 5. **Note** If required services, such as SNMP and WMI, are not running on the computer you are discovering, you may see a severity 15 event. If you see this type of event, see the detail message for more information about what caused the discovery to fail.

NetworkDevice

Use this Knowledge Script to discover network resources such as routers, switches, and gateways using a proxy architecture and `SNMP GET` commands. On successful discovery, any or all of the following devices are displayed in the TreeView pane of the Operator Console:

- Chassis resources: CPU, memory, flash memory, backplane, power supplies, fans, temperature sensors, and voltage sensors
- IP subsystem
- Host resource
- Interfaces: IP address and queue
- WAN links, serial links, frame relay links, and ATM links
- NetIQ SNMP Trap Receiver. For more information, see the Help for the **NetworkDevice_SNMPTrap_Async** Knowledge Script.

Ensure that all devices you want to discover have unique names. AppManager cannot differentiate between two IP addresses that have the same value for the `sysName` object, which is a name for a managed node assigned by an administrator, usually the hostname. When two devices have the same `sysName` object, AppManager assumes the two devices are the same single device. The list of devices you can monitor will be inaccurate if you do not assign unique names to your devices.

Configuring SNMP Permissions for Network Devices

Before using this script, you must configure SNMP information in AppManager Security Manager for each network device you want to monitor. The type of information you configure varies according to the version of SNMP that is implemented on the network device. AppManager for Network Device supports SNMP version 1, 2, and 3. SNMP v2 and SNMP v2c are essentially equivalent. All instructions for v2 are applicable for v2c.

If you do not specify an SNMP version, then AppManager attempts to determine the version during the Discovery job. This process could be quite time consuming.

Configuring SNMP information provides AppManager the permissions it needs to access the MIBs (management information bases) on SNMP-enabled network devices.

Configuration for SNMP Versions 1 and 2

You need to configure community string and version information for each network device that is being monitored by each proxy computer.

Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`NetworkDevice`
Sub-label	Indicates whether the user name and context you are configuring will be used for a single device or for all devices. • *For a single device* on a particular proxy agent computer, enter <*`device name`*>. • *For all devices* on a particular proxy agent computer, enter `default`.
Value 1	The appropriate read-only community string value, such as `private` or `public`.

Field	Description
Value 3	• `v1` or `1` if the device supports SNMPv1. • `v2` or `2` if the device supports SNMPv2. If you do not specify either SNMP version, AppManager attempts to determine the version during the Discovery job. This process can be quite time consuming.

Configuration for SNMP Version 3

AppManager for Network Devices supports the following modes for SNMP version 3 (SNMP v3):

- No authentication; no privacy
- Authentication; no privacy
- Authentication and privacy

In addition, the module supports the following protocols for SNMP v3:

- MD5 (Message-Digest algorithm 5, an authentication protocol)
- SHA (Secure Hash Algorithm, an authentication protocol)
- DES (Data Encryption Standard, encryption protocol)

Your SNMP v3 implementation may support one or more combinations of mode and protocol. That combination dictates the type of information you configure in AppManager Security Manager: user name (or entity), context name, protocol name, and protocol passwords.

You need to configure SNMP v3 information for each network device that is being monitored by each proxy computer.

Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`NetworkDevice`
Sub-label	Indicates whether the user name and context you are configuring will be used for a single device or for all devices. • *For a single device* on a particular proxy agent computer, enter <*`device name`*>. • *For all devices* on a particular proxy agent computer, enter `default`.
Value 1	The appropriate read-only community string value, such as `private` or `public`. All SNMP v3 modes require an entry in the **Value 1** field.
Value 2	The name of a context associated with the user name or entity you entered in the Value 1 field. A context is a collection of SNMP information that is accessible by an entity. If possible, enter a context that provides access to all MIBS for a device. If the device does not support context, type an asterisk (*). All SNMP v3 modes require an entry in the **Value 2** field.

Field	Description
Value 3	The combination of protocol and password appropriate for the SNMP v3 mode you have implemented. • For *no authentication/no privacy mode*, leave the **Value 3** field blank. • For *authentication/no privacy mode*, enter `md5` or `sha` and the password for the protocol, separating each entry with a comma. For example, enter `md5,abcdef` • For *authentication/privacy mode*, enter `md5` or `sha` and the associated password, and then enter `des` and the associated password, separating each entry with a comma. For example, enter `sha,hijklm,des,nopqrs`

Resource Object

You should only have one computer acting as a proxy for any given network device. Therefore, run this script on only one computer at a time.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the **Values** tab parameters as necessary.

Parameter	How to Set It
Auto Discovery	
Default gateway router	Enter the IP network address of the gateway (router) to query during discovery. **Note** Use this parameter if you are not certain of all the relevant subnets that should be scanned during discovery. If you enter an IP address here, AppManager will query the gateway for its routing tables and then attempt to discover every device in the tables.
Maximum number of hops	Enter the maximum number of hops that you want discovery to make during auto-discovery. Discovery considers the gateway router itself to be the first hop. Therefore, a *Maximum number of hops* setting of 1 means you will discover only the networks directly connected to the gateway router, and no other routers.
Walk subnets for layer-2 devices?	Set to n to discover all routers (Layer-3 devices) and all Cisco switches (Layer-2 devices), within the number of *Maximum number of hops* you have set, by means of routing tables and Cisco Discovery Protocol. Set to **y** to also discover all non-Cisco switches and other network devices, within the number of *Maximum number of hops* you have set, by means of a range discovery on all discovered subnets. **Caution** Set this parameter to **y** only with the understanding that walking the subnets for Layer-2 devices is an extremely time- and resource-intensive undertaking that can have a negative impact on your network's performance.

Parameter	How to Set It
List of network devices (comma-separated)	Specify a list of the network devices for which you want to discover resources. You must specify at least one network device. Use a comma to separate the names in the list. For example: `raldbellijm02,raldattixlm` You can enter hostnames or IP addresses. **Note** The community string information for each device that you list in this field must be configured in AppManager Security Manager before you can run this script.
List of network device ranges (comma-separated)	Specify a list of IP address ranges for the network devices for which you want to discover resources. Spaces are invalid in the list. Only numbers, dashes, periods, and commas are allowed. For example: `10.0.1.1-10.0.1.254,10.0.4.1-10.0.4.254` **Note** Limit the number of IP addresses in each range to no more than 256. To scan more than 256 IP addresses, break a range into multiple ranges, each with no more than 256 IP addresses.
Full path to file with list of network devices	Instead of identifying each network device separately, you can specify the full path to a file on the agent computer that contains a device name on each line of the file. **Note** The community string information for each of the network devices listed in the file must be entered into Security Manager before you can run this script.
Discovery Details	
Discover individual … … interfaces? … LAN links? … WAN links? … frame relay links? … ATM links? … FXS ports? … FXO ports? … ISDN channels?	This script will automatically discover interfaces, links, and ports when these parameters are set to **y** (which is the default setting). The default is y. **Note** To improve console performance, set these parameters to **n** for any device that you are not interested in monitoring. By not displaying these objects in the TreeView pane, you will significantly speed discovery and improve the performance of the TreeView pane of the Operator Console.
Trap Receiver Discovery	
Discover Trap Receiver?	Set to **y** to discover NetIQ SNMP Trap Receiver. The default is y.
Trap Receiver IP address	Specify the IP address of the computer on which Trap Receiver is installed. The default is `localhost`.
Trap Receiver TCP port	Specify the TCP port number through which Trap Receiver will communicate with AppManager. The default is port 2735.
Discover IP addresses that belong to the same device?	Set to **y** to discover all IP addresses for a single device. The same device will appear in the TreeView once for each different associated IP address. Set to **n** to discover a device only once, regardless of the number of associated IP addresses. Note that the number of discovered devices directly affects the number of licenses required for the AppManager for Network Devices module. The default is n.

Parameter	How to Set It
Discovery timeout	Enter the number of minutes that the script should attempt discovery before stopping as unsuccessful. The default is 10 minutes. The maximum is 60 minutes.
Raise event when discovery succeeds? (y/n)	This script always raises an event when discovery fails for any reason. In addition, you can set this parameter to **y** to raise an event when discovery succeeds.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.

NetWorker

Use this Knowledge Script to discover Legato NetWorker servers and the services and other resources (such as backup groups and devices) associated with those servers.

Resource Objects

Legato NetWorker server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have NetWorker installed. The default is 15 (yellow event indicator).

Networks-RT

Use this Knowledge Script to discover if AppManager ResponseTime for Networks components are available on a specific managed client. At the Operator Console, drag this Knowledge Script to the managed client on which you are performing discovery. This single Knowledge Script can discover either a Client (the default) or a Server.

After successful discovery, a new thumbnail appears in the TreeView pane with a list of servers that support it. Also, a new Networks-RT Knowledge Script pane will appear.

Resource Objects

Windows XP, Windows 2000, Windows NT or Windows Server 2003.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can select the **Yes** check box to raise an event when the job succeeds. By default, events are not raised on success.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator).

Networks-RTProxy

Use this Knowledge Script to discover remote computers, i.e. endpoints installed on UNIX computers and other places where a Windows-based AppManager agent and ResponseTime for Networks managed object cannot be installed, or where you don't want to install them. This Knowledge Script returns information about successful, failed and partial discoveries and raises events to notify you of errors.

This Knowledge Script discovers Network ResponseTime resources that will be used via a proxy computer. You may specify a list of computers separated by commas, or you may specify the name of a file that contains a computer name on each line of the file. The listed computers must be running the NetIQ Network Performance Endpoint version 4.5 or later.

You must specify at least one remote computer. You should only have one computer acting as a proxy for a given remote computer. Therefore, you may drop this Knowledge Script on only one computer at a time.

This Knowledge Script is similar to other AppManager Discovery Knowledge Scripts in that it discovers the resource objects on the computer where you run the discovery. with one important difference. However, this Knowledge Script also discovers the list of remote computers you specify in a configuration file. The computer where you run this Knowledge Script then becomes a proxy computer for contacting and monitoring the specified remote computers. By running this Knowledge script on a computer that will act as a proxy computer, you can monitor other computers that do not have the ResponseTime for Networks managed object or the AppManager agent installed.

Note
Each remote computer must only be monitored through one proxy computer. If you attempt to monitor a computer through multiple proxy computers, network connection tests may be executed multiple times, generating unneeded network traffic.

Resource Objects

Windows XP, Windows 2000, Windows NT or Windows Server 2003.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
List of remote computers	Specify a comma-separated list of remote computers.

Local path to file with list of computers	Specify the local full path or click **...** and select the local file containing a list of computer names. The format of the file is a list of computer names, one on each line. For example:
	`AJAX.EUROPE.CORP`
	`ACHILLES.EUROPE.CORP`
	`ATHENA.EUROPE.CORP`
	The file must be accessible from the proxy computer.

Additional list of remote computers (read from specified file)	This parameter only appears on the Web console and can be ignored.

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can select the **Yes** check box to raise an event when the job succeeds. By default, events are not raised on success.
Event severity when Discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator).

NortelBCM

Use this Knowledge Script to discover the Nortel BCM (Business Communications Manager) configuration information and resources.

Resource Objects

NT_MachineFolder

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.

NortelBCMx

Use this Knowledge Script to discover Nortel BCM resource and configuration information for BCM software version 4.0 and hardware models 50, 50a, 50e, 200, 400, and 1000.

AppManager for Nortel BCMx provides limited support for SRG (Survivable Remote Gateway) mode and local mode with the Alarms, CallByCallLimits, ChassisUsage, HealthCheck, HuntGroupUsage, InterfaceHealth, LinkUtilization, PSTNFallback, SystemUptime, and SystemUsage Knowledge Scripts. For more information, see the Help for those scripts.

Username and Password Configuration

Do not use this script until you have configured your BCM user name and password into AppManager Security Manager. The discovery process will fail if it cannot access this vital information.

AppManager cannot communicate with the Nortel BCM CIM server unless it has permission to do so. You can grant that permission by configuring the appropriate user name and password into AppManager Security Manager. Without knowing the user name and password, the discovery process cannot locate your BCM.

To configure Security Manager:

1. From the AppManager Operator Console, click **Security Manager** on the Extensions menu.
2. In the Tree pane, select the proxy agent computer for which you want to configure the user name and password.
3. On the Custom tab, click **Add**.
4. In the **Label** field, type `NortelBCMx`.
5. In the **Sub-Label** field, type `default`.
6. In the **Value 1** field, type your `[user name]`.
7. In the **Value 2** field, type your `[password]`.
8. Select **Extended application support** to encrypt the password when it is stored in the repository.
9. Click **OK**.
10. Repeat steps 2-9 to add user names and passwords for each additional proxy agent computer.
11. When done, close Security Manager.

Resource Objects

NT_MachineFolder

Default Schedule

By default, this script runs **once a week on Sunday at 3 A.M**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which this Knowledge Script job fails. The default is 5.
Raise event if discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **Yes** to raise an event when the job succeeds. The default is unchecked.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds in finding Nortel BCMx resources. The default is 25.
Raise event if discovery fails?	Set to **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails to find Nortel BCMx resources. The default is 5.
Raise event if Nortel BCMx agent not installed?	Set to **Yes** to raise an event if the Nortel BCMx agent is not installed. The default is Yes.
Event severity when Nortel BCMx agent not installed	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the Nortel BCMx agent is not installed. The default is 15.
Discover Nortel BCMx Devices	
List of Nortel BCMx devices	Use this parameter if you have only a few Nortel BCMx devices to discover. Enter a list of the devices for which you want to discover resources. Use a comma to separate the names or IP addresses in the list. For example: `10.0.1.1,10.0.4.1`.
List of Nortel BCMx device ranges	Use this parameter if you have only a few ranges of Nortel BCMx devices to discover. Enter a list of IP address ranges (up to 256 addresses) of the devices for which you want to discover resources. Only numbers, dashes, periods, and commas are allowed in the list. Dashes define a range. For example: `10.0.1.1-10.0.1.50, 10.0.4.51-10.0.4.100`
Full path to file with list of Nortel BCMx devices	Instead of listing each Nortel BCMx device separately, you can specify the full path to a file on the agent computer that contains a device name on each line of the file.

NortelBCM50x

Use this Knowledge Script to discover Nortel BCM resource and configuration information for BCM software version 4.0 and hardware models 50, 50a, 50e, 200, 400, and 1000.

Username and Password Configuration

Do not use this script until you have configured your BCM user name and password into AppManager Security Manager. The discovery process will fail if it cannot access this vital information.

AppManager cannot communicate with the Nortel BCM CIM server unless it has permission to do so. You can grant that permission by configuring the appropriate user name and password into AppManager Security Manager. Without knowing the user name and password, the discovery process cannot locate your BCM.

To configure Security Manager:

1. From the AppManager Operator Console, click **Extensions > Security Manager**. Security Manager opens.
2. In the Tree pane, select the computer for which you want to configure the user name and password. This computer will act as the proxy for the Nortel BCM device.
3. In the main body of Security Manager, click the **Custom** tab and then click **Add**. The Add Custom Entry dialog box is displayed.
4. In the **Label** field, enter `NortelBCM50x`.
5. In the **Sub-Label** field, enter `default`.
6. In the **Value 1** field, enter `[user name]`.
7. In the **Value 2** field, enter `[password]`.
8. Click to check **Extended application support**. This setting ensures that the password is encrypted when it is stored in the repository.
9. Click **OK**. The Label and Sub-label are displayed in the list.
10. Repeat steps 2-9 to add user names and passwords for each additional proxy computer.
11. When done, close Security Manager.

Resource Objects

NT_MachineFolder

Default Schedule

By default, this script runs **once a week on Sunday at 3 A.M**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance when this Knowledge Script job fails. The default is 40.
Raise event if discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **Yes** to raise an event when the job succeeds. The default is unchecked.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance when discovery succeeds. The default is 25.
Raise event if discovery fails?	Set to **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance when discovery fails. The default is 5.
Raise event if Nortel BCM50x agent not installed?	Set to **Yes** to raise an event if the Nortel BCM50x agent is not installed. The default is Yes.
Event severity when Nortel BCM50x agent not installed	Set the event severity level, from 1 to 40, to reflect the importance when the Nortel BCM50x agent is not installed. The default is 15.
Discover Nortel BCM50x Devices	
List of Nortel BCM50x devices	Use this parameter if you have only a few Nortel BCM50x devices to discover. Enter a list of the devices for which you want to discover resources. Use a comma to separate the names or IP addresses in the list. For example: `10.0.1.1,10.0.4.1`.
List of Nortel BCM50x device ranges	Use this parameter if you have only a few ranges of Nortel BCM50x devices to discover. Enter a list of IP address ranges (up to 256 addresses) of the devices for which you want to discover resources. Only numbers, dashes, periods, and commas are allowed in the list. Dashes define a range. For example: `10.0.1.1-10.0.1.50, 10.0.4.51-10.0.4.100`
Full path to file with list of Nortel BCM50x devices	Instead of listing each Nortel BCM50x device separately, you can specify the full path to a file on the agent computer that contains a device name on each line of the file.

NortelCC

Use this Knowledge Script to discover Nortel Contact Center servers and resources: applications, CDNs, databases, DNISs, IVR queues, and IVR ports.

Prerequisite

Before you can successfully discover Nortel Contact Server resources, configure AppManager Security Manager with the username and password that provide access to the Blue database.

Complete the following fields in the Custom tab of Security Manager for the SCCS computer.

Field	Description
Label	`NortelCC`
Sub-label	`DBLogin`
Value 1	`sysadmin`, which is the username that provides access to the Blue database. Some NortelCC installations may have other valid username/password combinations, but `sysadmin` will work on most systems.
Value 2	Password associated with the username specified in the **Value 1** field.
Value 3	Use this field *only* if you have used Cisco CallManager Administration to change the number of the HTTPS port the proxy agent computer uses to connect to the CallManager server. In the **Value 3** field, type the new secure port number. Leave this field blank to use the default port number: 8443.
Extended application support	Required field. Encrypts the password in Security Manager.

Resource Object

NT_MachineFolder

Default Schedule

By default, this script runs **once** every day.

Setting Script Parameters

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_NortelCC job fails. The default is 5.
Discovery Failure Notification	
Raise event if SQL query fails?	Set to **Yes** to raise an event if the SQL query fails. The default is Yes. Discovery_NortelCC uses a SQL query to retrieve Nortel Contact Center configuration information from the Blue database.

Parameter	How to Set It
Event severity when SQL query fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the SQL query fails to discover database configuration information. The default is 15.
Raise event if Registry read fails?	Set to **Yes** to raise an event if AppManager cannot read the Registry to search for the Nortel CC ELAN and CLAN IP addresses. The default is Yes.
Event severity when Registry read fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which AppManager cannot read the Registry. The default is 5.
Raise event if discovery succeeds?	Set to **Yes** to raise an event when discovery succeeds. The default is Yes.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.

NortelCS

Use this Knowledge Script to discover the various components of a Nortel CS1000 IP telephony system installation: Call Server, Signaling Server, Media Gateway Controller, Network Routing Server, MC32S, Enterprise Common Manager, and Voice Gateway Media Card.

This script also discovers co-resident Call Servers, Signaling Servers, and Element Managers. When co-resident, these components are installed on a single processor.

For Nortel CS1000 version 6.0 environments, this script discovers Bandwidth Management Zone (BMZ) objects on the Call Server. For earlier versions of Nortel CS1000, BMZ objects are discovered on the Signaling Server..

Before running discovery, ensure you have met all system requirements, which include the installation of several Nortel patches and identification of ELAN addresses for devices you want to monitor. Configuration needs vary depending on the version of Nortel CS1000 in use in your environment.

At the very least, you must enable SNMP access of Nortel CS1000 devices.

Prerequisite

To enable AppManager to use SNMP to access Nortel CS1000 devices, configure the SNMP community strings in AppManager Security Manager *before* you discover Nortel CS1000 devices.

Use the following procedure to configure your community strings for one or more variations:

- If your read-only community string information is the same for all Nortel CS1000 devices, complete the following procedure once, using the `default` **Sub-label**.
- If your read/write community string is the same for all Signaling Servers, MGMCs, MGCs, and MC32Ss, complete the following procedure once, using the `default write` **Sub-label**.
- If your read-only or read/write community string information is different for different devices, complete the following procedure once for each different community string, using the device's ELAN IP address as the **Sub-label**.

Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`NetworkDevice`
Sub-label	• For all devices that use the **same read-only** community string, enter `default`. Use the `default` sub-label for the read-only community string used on the greatest number of devices. • For all devices that use the **same read/write** community string, enter `default write`. Use the `default write` sub-label for all Signaling Server, VGMC, MGC, and MC32S devices that use the same read/write community string. • For a single device that uses a **unique read-only** community string, enter <*`IP address`*>, where <*`IP address`*> is the ELAN IP address of the Call Server, Media Gateway, NRS, or ECM device. • For a single device that uses a **unique read/write** community string, enter <*`IP address`*> `write`, where <*`IP address`*> is the ELAN IP address of the Signaling Server, VGMC, MGC, or MC32S device.

Field	Description
Value 1	• To monitor a Call Server, Media Gateway (Nortel CS1000 version 4.50 and earlier), Network Routing Server, or Enterprise Common Manager, enter your **configured read-only community string**. • To monitor a Signaling Server, VGMC, Media Gateway Controller, or MC32S, enter your **configured read/write community string**. The read/write community string provies SNMP access to the MIBs on these devices.

The following are examples:

- If you are monitoring multiple Signaling Servers that have the same read/write community string, type `default write` in the **Sub-label** field and type the read/write community string in the **Value 1** field.
- If you are monitoring a Call Server that has a unique read-only community string, type the ELAN IP address of the Call Server in the **Sub-label** field and type the read-only community string in the **Value 1** field.
- If you are monitoring a VGMC that has a unique read/write community string, type `<IP address write>` in the **Sub-label** field (where `<`*`IP address`*`>` is the ELAN IP address of the VGMC) and type the read/write community string in the **Value 1** field.

Resource Object

Windows server

One computer can act as proxy for multiple Nortel CS1000 systems. However, each system should have only one proxy. NetIQ Corporation does not recommend establishing multiple proxies per system.

Default Schedule

By default, this script runs weekly, on Sundays at 3 A.M. The default schedule allows the discovery process to run at a time that is probably less busy for your Call Server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if discovery fails?	Set to **Yes** to raise an event if discovery fails for any reason. The default is Yes.
Event severity if discovery fails	Set the event severity level, from 1 to 40, to reflect the importance when discovery fails. The default is 5.
Raise event if discovery partially succeeds?	Set to **Yes** to raise an event if discovery is partially successful. A partially successful discovery is one in which, for example, AppManager can discover devices but cannot create an inventory report. Or one in which, for example, AppManager can discover all Signaling Servers, but not the Bandwidth Management Zones. The default is Yes.
Event severity if discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance when discovery is partially successful. The default is 15.

Parameter	How to Set It
Raise event if discovery succeeds?	Set to **Yes** to raise an event if discovery succeeds. The default is unchecked.
Event severity if discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance when discovery succeeds. The default is 25.
Call Server	Provide the hostname or IP address of the Nortel CS1000 Call Server, such as `CS1000_CS`. Do not enter the IP address or hostname of the Call Server that is part of the Media Gateway. **Important** Provide *only* one Call Server hostname or IP address. Discovery is meant to discover only one Nortel CS environment.
List of NortelCS devices	Use this parameter if you know which Nortel CS1000 devices you want to discover. Type a list of the devices you want to discover. Use a comma to separate the names in the list; for example: `CS1000_VGMC,CS1000_SS`. You can type hostnames (if you use DNS in your environment) or ELAN IP addresses. **Notes** • Leave this field blank if you only want to discover the Call Server, which you identified in the previous parameter. • The community string information for each device you list in this field must be configured in Security Manager before you run this script.
List of NortelCS device ranges	Type a list of ELAN IP address ranges for the Nortel CS1000 devices you want to discover. Spaces are invalid in the list; only numbers, dashes, periods, and commas are allowed. For example: `10.0.1.1-10.0.1.254,10.0.4.1-10.0.4.254`. **Notes** • Leave this field blank if you only want to discover the Call Server, which you identified in the *Call Server* parameter. • Limit the number of IP addresses in each range to no more than 256. To scan more than 256 IP addresses, break a range into multiple ranges, each with no more than 256 IP addresses.
Full path to file with list of NortelCS devices	Instead of listing each Nortel CS1000 device separately, you can specify the full path to a file on the agent computer that contains a device name on each line of the file. **Notes** • Leave this field blank if you only want to discover the Call Server, which you identified in the *Call Server* parameter. • The community string information for each device listed in the file must be configured in Security Manager before you run this script.

Parameter	How to Set It
Discovery timeout	Specify the amount of time (no more than 60 minutes) the script should attempt discovery before stopping as an unsuccessful discovery. The default is 10 minutes.
Discover phones using the Call Server's Entity MIB?	Set to **Yes** to use the Entity MIB (management information base) to count IP phones for the inventory report. AppManager will perform an SNMP query of this Call Server MIB to retrieve the inventory results. This parameter is applicable **only** for Nortel CS1000 4.0 and later. Uncheck the box if you use Nortel CS1000 3.0. **Important** Issue the following Overlay 117 commands before running discovery. LD 117 INV MIDNIGHT SETS INV ENTITY SETS ON

NortelCS2x

Use this Knowledge Script to create the Nortel CS2x supplemental database and to configure the services that collect data from Nortel CS2000 or CS2100 components:

- Integrated Element Management System (IEMS)
- Element Managers
- Centrex IP Call Managers (CICM)

The following is a brief summary of the architecture for AppManager for Nortel CS2x.

- Individual Element Managers and the Core and Billing Manager (CBM) send logs and OM Reports to the IEMS (Integrated Element Management System), which in turn sends the logs to the log collector service and the OM Reports to the OM file collector service over Telnet. The log collector service listens on port 8555. The OM file collector service listens on port 22.
- The CBM constructs end-of-call QoS Collector Application records from per-call information published by gateway controllers. It then uses sFTP to send these records to the QoS file collector service.
- The CICM Element Manager sends syslogs to the QoS syslog collector service.
- The NortelCS2x_CollectorHealth Knowledge Script verifies that all collectors are installed and contain data. And, by issuing commands stored in the CMD table in the supplemental database, the CollectorHealth script prompts the collector services to push their data to the supplemental database using Open Database Connectivity (ODBC).
- The NortelCS2x_CallActivity, NortelCS2x_CallFailures, NortelCS2x_CallQuality, NortelCS2x_LogQuery, NortelCS2x_OMQuery, NortelCS2x_PhoneInventory, and NortelCS2x_PhoneQuality Knowledge Scripts query the supplemental database for the information you specify.

Configuring Nortel CS2100 to Work with AppManager

The following table describes the configuration tasks that, when completed, allow the Nortel CS2100 switch to work with AppManager and the AppManager for Nortel CS2100 module.

Requirement	Description
Read-only login account (user name and password) to sFTP on the IEMS	• Contact your Nortel CS2100 administrator to create this account. For more information, see Nortel document NN10336-611: *Carrier VoIP: IEMS Administration and Security*. • Configure the read-only user name and password in AppManager Security Manager.

Requirement	Description
Set up log destination	On the IEMS (Integrated Element Management System), configure the proxy agent computer's IP address as a log destination. For more information, see Nortel document NN10334-911: *Integrated EMS Fault Management*. 1. At the IEMS, navigate to the Runtime Administration window. 2. In the tree pane, expand the **Categories** folder and select the **NTSTD** node. 3. In the **Manager Host** field, provide the proxy agent computer IP address. 4. In the **Office Identifier** field, provide the office identifier of the CS2100 switch. As a best practice, use the same identifier you use in the *Unique identifier of the switch to discover* parameter in the Discovery_NortelCS2x Knowledge Script. 5. Click **Add** and then click **Apply**. **Notes** • If the proxy agent computer is outside the firewall, configure the firewall address rather than the proxy agent computer address. • Ensure TCP port 8555 (the NTSTD port) is open on the firewall between the proxy agent computer and the IEMS.
Set up OM Report collection	• Set up an FTP dropbox server that supports both FTP and sFTP. • On the CBM (Core and Billing Manager), configure the FTP server as a "file transfer destination." For more information, see Nortel document NN10148-711: *Carrier VoIP: Nortel CS2000 Core Manager Performance Management*. • On the CBM, add the following OM Report groups to a report element: SITE, PM, LMSD, TRK, CP, SITE2, XPMOVLD. For more information, see Nortel document NN10148-711: *Carrier VoIP: Nortel CS2000 Core Manager Performance Management*.
Enable QoS reporting	Setup QoS collection at the GWC (gateway controller) Element Manager. For more information, see Nortel document NN10240-511: *Carrier VoIP: Nortel CICM Configuration*. 1. Access the CS2000 Management Tools application. 2. Expand the **Device Types** folder and select **Gateway Controller**. 3. In the Gateway Controllers panel, select the GWC you want to configure. 4. On the QoS Collectors tab, select **Enable QoS Collection**. 5. On the File menu, select **Save**.
Enable syslog delivery	Configure the proxy agent computer as the destination for the CICM syslogs. 1. Access the Centrex IP Client Manager and navigate to the Global Settings Modification page. 2. On the Global tab, provide the proxy agent computer IP address in the **Extended QoS server Ip Address** field. 3. In the **Extended QoS server port** field, provide the port number on the proxy agent computer that will listen for syslogs. Enter the same port number you use in the *Port number to receive QoS syslog messages on* parameter in the Discovery_NortelCS2x Knowledge Script. In the Discovery script, port 514 is the default port number. If port 514 is in use, select another port number and ensure you indicate the same port number in the Discovery script.

Requirement	Description
Enable delivery of voice quality alerts	Create a Voice Quality Monitoring (vqmon) profile on the CICM Element Manager. The vqmon profile allows AppManager to receive the alerts monitored by the NortelCS_CallAlert Knowledge Script. 1. Access the Centrex IP Client Manager and navigate to the vqmon Profiles page. 2. In the **Profile name** field, enter `netiq`. 3. Accept the **Default Value** for all other fields. 4. Click **save your changes to this profile**.

Prerequisites

Configure AppManager Security Manager with the user names and passwords of the CS2100 components you want to monitor.

For a remote supplemental database, prepare the remote computer for creation of the supplemental database.

Configuring CICM User Names and Passwords in Security Manager

The NortelCS2x_RetrieveConfigData Knowledge Script retrieves station configuration information from individual CICM Element Managers. Before running the RetrieveConfigData Knowledge Script, configure AppManager Security Manager with the user name and password of the CICM Element Manager. This information allows AppManager to access the configuration information in the Element Managers.

On the Custom tab in Security Manager, complete the following fields:

Field	Description
Label	`NortelCS2x_CICM-EM`
Sub-label	The name of the switch associated with the Element Manager. This is the same information you provide in the *Unique identifier of the switch to discover* parameter in the Discovery_NortelCS2x Knowledge Script. Or, type `default` if the user name and password apply to all switches.
Value 1	The Element Manager user name.
Value 2	The Element Manager password.
Extended application support	Encrypts the user name and password in Security Manager. Do not leave this option unselected.

Configuring sFTP User Names and Passwords in Security Manager

The OM file collector service and QoS file collector service receive data over secure FTP (sFTP). Before you run the Discovery_NortelCS2x Knowledge Script, configure AppManager Security Manager with the user name and password of the associated sFTP server.

On the Custom tab in Security Manager, complete the following fields:

Field	Description
Label	• For the OM file collector service, `NortelCS2x_OMFileCollector` • For the QoS file collector service, `NortelCS2x_QoSFileCollector`
Sub-label	The name of the switch associated with the sFTP server. This is the same information you provide in the *Unique identifier of the switch to discover* parameter in the Discovery_NortelCS2x Knowledge Script. Or, type `default` if the user name and password apply to all switches.
Value 1	The sFTP user name.
Value 2	The sFTP password.
Extended application support	Encrypts the user name and password in Security Manager. Do not leave this option unselected.

Configuring SQL Server User Names and Passwords in Security Manager

The Discovery_NortelCS2x and SetupSupplementalDB Knowledge Scripts require access to the SQL Server database on the remote computer on which you want to install the Nortel CS2x supplemental database. Before you run the Discovery or SetupSupplementalDB scripts, configure AppManager Security Manager with the user name and password of the remote SQL Server computer.

On the Custom tab in Security Manager, complete the following fields:

Field	Description
Label	`NortelCS2x_Database`
Sub-label	The unique, common name of the CS2x office that contains the remote computer on which you want to create the Nortel CS2x supplemental database. Use the same name you entered in the *Unique identifier of the switch to discover* parameter in the Discovery_NortelCS2x Knowledge Script. `Default` is an acceptable value for this parameter.
Value 1	The SQL Server user name for the remote computer on which you want to create the Nortel CS2x supplemental database.
Value 2	The SQL Server password associated with the user name you supplied in the Value 1 field.
Extended application support	Encrypts the user name and password in Security Manager. Do not leave this option unselected.

Configuring the Remote Supplemental Database Computer

Take the following steps to prepare a SQL Server computer for creation of the remote supplemental database.

To set up the remote SQL Server computer:

1. Use SQL Server Configuration Manager to disable dynamic ports.
2. Use SQL Server Configuration Manager to enable TCP/IP on the instance object where you want to create the remote supplemental database.

3. Use Microsoft SQL Server Management Studio to enable **SQL Server** and **Windows Authentication mode** on the instance object where you want to create the remote supplemental database.
4. Create a new SQL Server user name and password. Assign the new user both `sysadmin` and `processadmin` privileges.
5. In AppManager Security Manager, configure the new user name and password.

Resource Object

Nortel CS2x

Only one computer can act as proxy for any given Communication Server cluster. Therefore, run this script on only one computer at a time.

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_NortelCS2x Knowledge Script job fails. The default is 5.
Raise event if discovery succeeds?	Select **Yes** to raise an event if the supplemental database is created and the collector services are configured. The default is Yes.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the supplemental database is created and the collector services are configured. The default is 25.
Raise event if discovery fails?	Select **Yes** to raise an event if the supplemental database is not created or the collector services are not configured. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the supplemental database is not created or the collector services are not configured. The default is 5.
Unique identifier of the switch to discover	Provide the unique, common name of the CS2100 office you want to discover. The common name is displayed in the logs created by the CS2100. As a best practice, the common name should match the office name in one of the following locations: • `LOG_OFFICE_ID` in the core table `OFCVAR` • `OFFICE_CLLI_NAME` • Office log name in the IEMS **Note** Do not leave this field blank.
IP address of the IEMS	Provide the IP address of the IEMS you want to discover.
Supplemental Database Creation	

Parameter	How to Set It
Set up supplemental database?	Select **Yes** to create the Nortel CS2x supplemental database, including the tables and stored procedures needed to store log files, OM Reports, call details, and QoS information. When the database is populated, you can monitor the data using the NortelCS2x_CallActivity, NortelCS2x_CallQuality, NortelCS2x_LogQuery, NortelCS2x_OMQuery, and NortelCS2x_PhoneQuality Knowledge Scripts. You can also create the supplemental database after you run the Discovery script. For more information, see the Help for the NortelCS2x_SetupSupplementalDB Knowledge Script.
Database Record Retention	
Number of days to keep supplemental database records	Specify the number of days you want to keep records in the Nortel CS2x supplemental database. Data older than that is discarded. The default is 14 days.
SQL Server Information	
SQL Server computer name	Specify the DNS name or IP address of the SQL Server computer on which you want to create the remote Nortel CS2x supplemental database. Leave this parameter blank to create the database on the computer on which you run this script. For either a remote or local supplemental database, configure the SQL Server user name and password in AppManager Security Manager.
SQL Server instance name	Specify the name of the SQL Server instance on the computer in which you want to create the Nortel CS2x supplemental database. Leave this parameter blank to accept the default instance name.
Raise event if database setup succeeds?	Select **Yes** to raise an event if creation of the Nortel CS2x supplemental database is successful. The default is unselected.
Event severity when database setup succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the success of the creation of the Nortel CS2x supplemental database. The default is 25.
Configuration Data Retrieval	
Retrieve configuration data from IEMS?	Select **Yes** to retrieve station configuration information from individual CICM Element Managers and store it in the Nortel CS2x supplemental database, where it can be monitored by the NortelCS2x_PhoneInventory Knowledge Script. You can also retrieve station configuration information after you run the Discovery script. Use the NortelCS2x_RetrieveConfigData Knowledge Script.
Log Collector Service	
Configure log collector service?	Select **Yes** to create and start the log collector service on the proxy agent computer. The default is Yes. Element Managers push logs to the log collector service over Telnet. Associated Knowledge Scripts are NortelCS2x_CallFailures, NortelCS2x_LogQuery, and NortelCS2x_OMQuery.
Server address to receive log messages from	Specify the IP address of the Element Manager that will send logs. Leave this field blank if the address is that of the IEMS.
Port number to receive log messages from	Specify the port number on the proxy agent computer that will listen for logs. The default port number is 8555.

Parameter	How to Set It
Time stamp offset for time zone differences on log messages	If your CS2100 office and proxy agent computer are in different time zones, use this parameter to adjust the time stamps on the logs sent by the CS2100. For example, if the time zone of your proxy agent computer is three hours *ahead* of the CS2100 that is sending logs, the difference in minutes is 180. So specify `180` in this parameter. If the time zone of your proxy agent computer is three hours *behind* that of your CS2100, specify `-180` in this parameter. **Note about Daylight Savings Time** You may need to manually adjust the time stamp offset at the Spring and Fall time change for Daylight Savings Time (DST). If your query Knowledge Script jobs (CallActivity, CallFailures, CallQuality, LogQuery, and OMQuery) return no data, but data has been collected and stored in the supplemental database, verify the time stamps in the data. If the time stamps have been affected by DST, rerun the Discovery script using a new time stamp offset value.
OM File Collector Service	
Configure OM file collector service?	Select **Yes** to create and start the OM file collector service on the proxy agent computer. The default is Yes. Element Managers send OM Reports to the IEMS, which in turn sends the OM Reports to the OM file collector service over sFTP. The associated Knowledge Script is NortelCS2x_CallActivity.
Server address to receive sFTP OM Reports from	Specify the IP address of the Element Manager that will send OM Reports over sFTP. Leave this field blank if the address is that of the IEMS.
Port number to receive sFTP OM Reports from	Specify the port number on the proxy agent computer that will listen over sFTP for OM Reports. The default port number is 22.
Directory location at sFTP server to retrieve sFTP OM Reports from	Specify the name of the directory on the sFTP server from which to retrieve the OM Reports. **Note** Do not leave this field blank.
Time stamp offset for time zone differences on sFTP OM Reports	If your CS2100 office and proxy agent computer are in different time zones, use this parameter to adjust the time stamps on the OM Reports sent by the CS2100. For example, if the time zone of your proxy agent computer is three hours *ahead* of the CS2100 that is sending OM Reports, the difference in minutes is 180. So specify `180` in this parameter. If the time zone of your proxy agent computer is three hours *behind* that of your CS2100, specify `-180` in this parameter. **Note about Daylight Savings Time** You may need to manually adjust the time stamp offset at the Spring and Fall time change for Daylight Savings Time (DST). If your query Knowledge Script jobs (CallActivity, CallFailures, CallQuality, LogQuery, and OMQuery) return no data, but data has been collected and stored in the supplemental database, verify the time stamps in the data. If the time stamps have been affected by DST, rerun the Discovery script using a new time stamp offset value.
QoS Syslog Collector Service	
Configure QoS syslog collector service?	Select **Yes** to create and start the QoS syslog collector service on the proxy agent computer. The default is Yes. The QoS syslog collector service receives end-of-call QoS syslogs from CICM Element Managers. The associated Knowledge Script is NortelCS2x_CallQuality.

Parameter	How to Set It
Server address to receive QoS syslog reports from	Specify the IP address of the Element Manager that will send QoS syslog reports. Leave this field blank if the address is that of the IEMS.
Port number to receive QoS syslog reports on	Specify the port number on the proxy agent computer that will listen for syslogs reports. The default port number is 514.
Time stamp offset for time zone differences on QoS syslog messages	If your CS2100 office and proxy agent computer are in different time zones, use this parameter to adjust the time stamps on the QoS records sent by the CS2100. For example, if the time zone of your proxy agent computer is three hours *ahead* of the CS2100 that is sending QoS records, the difference in minutes is 180. So specify `180` in this parameter. If the time zone of your proxy agent computer is three hours *behind* that of your CS2100, specify `-180` in this parameter. **Note about Daylight Savings Time** You may need to manually adjust the time stamp offset at the Spring and Fall time change for Daylight Savings Time (DST). If your query Knowledge Script jobs (CallActivity, CallFailures, CallQuality, LogQuery, and OMQuery) return no data, but data has been collected and stored in the supplemental database, verify the time stamps in the data. If the time stamps have been affected by DST, rerun the Discovery script using a new time stamp offset value.
QOS File Collector Service	
Configure QoS file collector service?	Select **Yes** to create and start the QoS file collector service on the proxy agent computer. The default is Yes. Element Managers send QoS files to the IEMS, which in turn sends the QoS files to the QoS file collector service over sFTP. The associated Knowledge Script is NortelCS2x_CallQuality.
Server address to receive QoS files from	Specify the IP address of the CBM that will send QoS files over sFTP. Leave this field blank if the address is that of the IEMS.
Port number to receive QoS files from	Specify the port number on the proxy agent computer that will listen over sFTP for QoS files. The default port number is 22.
Directory location at sFTP server to receive active QCA file	Specify the name of the directory on the sFTP server from which to retrieve the QoS Collector Application file containing the QoS data. **Note** Do not leave this field blank.
Time stamp offset for time zone differences on sFTP QoS reports	If your CS2100 and proxy agent computer are in different time zones, use this parameter to adjust the time stamps on the QoS records sent by the CS2100. For example, if the time zone of your proxy agent computer is three hours *ahead* of the CS2100 that is sending QoS reports, the difference in minutes is 180. So specify `180` in this parameter. If the time zone of your proxy agent computer is three hours *behind* that of your CS2100, specify `-180` in this parameter. **Note about Daylight Savings Time** You may need to manually adjust the time stamp offset at the Spring and Fall time change for Daylight Savings Time (DST). If your query Knowledge Script jobs (CallActivity, CallFailures, CallQuality, LogQuery, and OMQuery) return no data, but data has been collected and stored in the supplemental database, verify the time stamps in the data. If the time stamps have been affected by DST, rerun the Discovery script using a new time stamp offset value.

NT

Use this Knowledge Script to discover Microsoft Windows configuration and resource information, including related resources such as network services.

This script discovers shared disks under the Cluster Alias object in the TreeView and local disks under regular Windows server objects.

Discover Windows resources before discovering clustered applications, if applicable in your environment. For more information, see Cluster.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when discovery succeeds?	Set to **y** to raise an event when discovery succeeds. The default is n. However, this script always raises an event when the job fails for any reason.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25 (blue event indicator).
Event severity when discovery is not applicable	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery is not applicable. This type of failure usually occurs when the target computer does not have a supported operating environment installed. The default is 15 (yellow event indicator).

OCS

Use this Knowledge Script to discover all known resources on an OCS server. The script discovers OCS Enterprise and Standard editions, Media servers, and Edge servers. When AppManager discovers an OCS component, that component displays under the relevant server in the tree view on the left-hand side of the AppManager window.

Before running discovery, ensure you have set up the proper user permissions on the various OCS servers and SQL servers you will be using. For more information, see "Setting up User Permissions for OCS" in the *NetIQ AppManager for Microsoft OCS Management Guide*.

Resource Objects

NT_MachineFolder

Default Schedule

The default interval for this script is weekly; the default is Sundays at 3 A.M.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the discovery job fails. The default is 5.
Raise event if discovery succeeds?	Set to **Yes** to raise an event when the discovery process is successful. The default is unchecked.
Event severity when discovery succeeds	If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25.
Raise event if discovery succeeds with warnings?	Set to **Yes** to raise an event when the discovery process is succeeds, but generates some warnings. The default is Yes.
Event severity when discovery succeeds with warnings	If you set this Knowledge Script to raise an event when the job succeeds, but with warnings, set the event severity level for a successful discovery. The default is 15.
Raise event if discovery fails?	Set to **Yes** to raise an event when the discovery process fails. The default is Yes.
Event severity when discovery fails	If you set this Knowledge Script to raise an event when the job fails, set the event severity level for a failed discovery. The default is 10.

Oracle

Use this Knowledge Script to discover configuration and resource information for Oracle database servers.

In order to successfully discover Oracle configuration and resource information, the account under which you run this Knowledge Script must have `SELECT` permissions for the following tables:

```
dba_data_files
dba_extents
dba_free_space
dba_rollback_segs
dba_segments
dba_tables
dba_tablespaces
dba_temp_files
dba_users
sys.fet$
sys.seg$
sys.ts$
v_$archive_dest
v_$bgprocess
v_$database
v_$datafile
v_$instance
v_$librarycache
v_$lock
v_$parameter
v_$process
v_$rowcache
v_$session
v_$sesstat
v_$statname
v_$sysstat
v_$thread
v_$version
```

Resource Objects

Oracle servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Username	Enter the username for logging on to the Oracle server. The username must have permission to access Oracle on the target computer(s). You can use the Security Manager to specify the user accounts that have access to specific computers. The default is the system user account.

Parameter	How to Set It
Raise event if discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator).

Oracle-RT

Use this Knowledge Script to discover if AppManager ResponseTime for Oracle components are available on a specific managed client. At the Operator Console, drag this Knowledge Script to the managed client on which you are performing discovery.

After successful discovery, a new thumbnail appears in the TreeView pane with a list of computers on which you are performing discovery.

Resource Objects

Windows XP Professional, Windows 2000, or Windows NT.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can select the **Yes** check box to raise an event when the job succeeds. By default, events are not raised on success.
Event severity when Discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **... fails**. The default is 5 (red event indicator). • **...is partially done**. This type of failure usually occurs when the target computer does not have all the prerequisites installed. The default is 10 (red event indicator).

OracleUNIX

Use this Knowledge Script to discover Oracle system resources on UNIX and Linux servers.

To successfully discover Oracle configuration and resource information, the account with which you run this Knowledge Script must have `SELECT` permissions for the following tables:

```
DBA_DATA_FILES
DBA_SEGMENTS
DBA_TABLESPACES
DBA_USERS
v$DATABASE
v$INSTANCE
v$VERSION
```

Resource Objects

UNIX/Linux machine folder

Default Schedule

The default interval for this script is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Oracle Username	Enter the Oracle username used to access the target databases. If you run this script on more than one computer, each database must be configured with the same username. **Note** To use SYSDBA authentication, leave the **Oracle Username** parameter blank. The default is blank.
Discover instances not automatically started upon system boot?	Set to Yes to discover Oracle instances not started by the `dbstart` utility upon system boot. This information is obtained from the `oratab` file. The default is Yes
Raise event when discovery fails?	Set to Yes to raise an event when discovery fails. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event when discovery partially succeeds?	Set to Yes to raise an event when discovery is partially successful. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 30.
Raise event when discovery succeeds?	Set to Yes to raise an event when discovery succeeds. The default is no.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 40.

PhoneQuality

Use this Knowledge Script to discover a Phone Quality object on the computer that will be used for monitoring Cisco IP phones. This script always raises an event when the job fails for any reason.

When polling a phone to get device information, the managed object has a 20-second timeout period for each phone that it is attempting to contact. If you are rediscovering a lot of phones at one time, it may take quite a while if phones cannot be contacted.

Resource Object

NT_MachineFolder

Default Schedule

By default, this script is only run **once** for each server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance when the discovery job fails. The default is 5.
Update phone details for existing phones?	Set to **Yes** to poll device information from phones already in the TreeView pane. The default is Yes.
Raise event if discovery succeeds?	Set to **Yes** to raise an event if discovery is successful. The default is Yes.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance when discovery succeeds. The default is 25.
Raise event if discovery fails?	Set to **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance when discovery fails. The default is 5.
Raise event if phone details cannot be updated?	Set to **Yes** to raise an event if discovery encounters an error during when polling one or more phones for device information. The default is Yes.
Event severity when phone details cannot be updated	Set the event severity level, from 1 to 40, to reflect the importance when phone details cannot be updated. The default is 15.
Raise event if Phone Quality managed object not installed?	Set to **Yes** to raise an event when the Phone Quality managed object is not installed. The default is Yes.
Event severity when Phone Quality managed object not installed	Set the event severity level, from 1 to 40, to reflect the importance when the Phone Quality managed object is not installed at the time the discovery job is run. The default is 5.

Proxy

This script is obsolete as of the release of AppManager version 7.0.

Use this Knowledge Script to discover Microsoft Proxy Server configuration and resources.

Resource Objects

Proxy servers

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have Proxy server installed. The default is 15 (yellow event indicator).

ReportAgent

Use this Knowledge Script to discover the NetIQ AppManager report agent and associated data sources.

Resource Objects

Any computer with the AppManager report-enabled agent installed.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Discovery Type	
Discover AppManager repository?	Set to **y** to discover the AppManager repository resource object. Successful discovery of this object allows you to run render reports based on data in the AppManager repository. The default is y.
Discover Active Directories?	Set to **y** to discover Active Directory resource objects. Successful discovery of Active Directories allows you to render reports based on the data contained therein. The default is n.
Event Notification	
Raise event if discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have the AppManager report agent installed. The default is 15 (yellow event indicator).

Notes

This Knowledge Script is currently not supported in the Web Console. It is recommended that you use it in the Operator Console.

The Action module provides the RunKS Knowledge Script to automatically run the scripts that you select. However, you cannot select the ReportAgent Knowledge Script to run automatically in the RunKS script. You need to manually run the ReportAgent Knowledge Script.

Re-running Discovery_ReportAgent

There are some circumstances under which you must run the Discovery_ReportAgent Knowledge Script again:

- If you add a new data source (for example, Active Directory).
- If you install new applications for which AppManager provides application-specific reports (for example, if you install Oracle).

If you add a new data source, re-running Discovery_ReportAgent adds it as a child of the report agent, and displays the corresponding Report Scripts in the Operator Console.

If you install a new application (and discover it), re-running Discovery_ReportAgent adds the discovered application to the appropriate AppManager repository under the report agent, and displays the corresponding application-specific reports.

When you run Discovery_ReportAgent again, be sure to set the Knowledge Script to discover existing data sources (for example, if you have previously discovered Active Directories, be sure to enable the **Discover Active Directories?** parameter). Failure to rediscover existing data sources will remove them from the report agent.

SAP

Use this Knowledge Script to discover SAP R/3 systems (application servers and database servers) in your environment. Before discovery, you must install the AppManager for SAP managed object (`qsapa`*`n`*`.dll`) and AppManager agent on the computer you want to use as the SAP proxy. After you install the agent and managed object, you must manually run this Knowledge Script on the managed client you are using as the proxy.

Note
You may need to restart the Operator Console after you discover SAP to refresh the cache and ensure the SAP resource objects are registered before starting SAP jobs.

Resource Objects

Windows computer acting as the SAP R/3 proxy server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Database name for SAP Proxy	Enter the name of the database on the computer you are using as the proxy for SAP R/3. The default is sapdb.
User name for SAP Proxy database (leave blank for NT authentication)	Enter the username for logging in to the database on the SAP proxy. Leave this field blank to use your current login user name and Windows user authentication.
SAP R/3 client number	Enter an SAP R/3 client number for logging in. There are three default clients in SAP R/3 that are always present —000, 001, and 066.
SAP R/3 user name	Enter an SAP R/3 user name with permission to access the SAP R/3 system. This name becomes the AppManager for SAP R/3 (AMSAP) **configuration name** you use to access login information. **Note** The SAP R/3 login information you enter for this Knowledge Script is required for a successful discovery. After the SAP R/3 systems are discovered, you can use this same login information to run any SAP Knowledge Script by typing the name you enter here in the AMSAP configuration name field.
SAP R/3 password	Enter the SAP R/3 password for the user. The default is netiq.
SAP R/3 login language	Enter the login language code to use. For example, EN for English.
SAP R/3 application server	Enter the name of the application server central instance host name. For example, mckinley.
SAP R/3 system number	Enter the system (port) number for the application server central instance. For example, 00.
NetIQ Corporation management server machine name	Enter the name of the AppManager management server computer to communicate with. For example, SHASTA.

Parameter	How to Set It
Discover custom CCMS alerts only?	Set to **y** to discover only the CCMS alerts tree that you have defined in SAP, and not the pre-defined alerts trees that come with SAP. If you have not yet defined your own CCMS alerts trees, you should set this parameter to n. The default is y. If you set this parameter to n, you must also set to n the parameter “Show user-defined CCMS alerts only?” in the AlertsAcknowledge and AlertsShowOpen Knowledge Scripts. If you do not, events will be raised against incorrect or non-existent objects.
Event for successful discovery	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity levels	Set the event notification level to give you the desired visibility for a successful, failed, or partially completed discovery. By default, the severity levels are: • Discovery was successful: severity 25 (blue event indicator) • Discovery failed: severity 5 (red event indicator) • Discovery was partially done: severity 15 (yellow event indicator)

SAPITS

Use this Knowledge Script to discover SAP Internet Transaction Servers and services.

Resource Objects

SAP Internet Transaction Servers.

Default Schedule

The default interval for this script is one time.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
SAP Internet Transaction Server (ITS) host name	Enter the SAP R/3 Internet Transaction Server host name. For example, MOON.
Event for successful discovery? (y/n)	Set to **y** to raise an event when discovery succeeds. The default is y.
Event severity when discovery...	Set the event severity level, from 1 to 40, to indicate the importance when: • **...succeeds.** The default is 25 (blue event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 15 (yellow event indicator). • **...fails**. The default is 5 (red event indicator).

ScanMailExch

Use this Knowledge Script to discover TrendMicro ScanMail for Exchange components on the computers in your network.

Resource Objects

ScanMail for Exchange servers.

Default Schedule

By default, this script is run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	Use the following parameters to raise events and set severity levels
Successful discovery event?	Select the **Yes** check box to raise an event if discovery succeeds. By default, this script does not raise an event under these circumstances.
Event severity if discovery...	Set the event severity level, from 1 through 40, to indicate the importance of the event when discovery: • **...succeeds**. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have ScanMail for Exchange installed. The default is 15 (yellow event indicator).

Security

Use this Knowledge Script to discover Microsoft Windows Security configuration and resources and to perform the following tasks:

- Identify computers with Windows security auditing disabled

  Windows security auditing enables the operating system to record security-specific events in the Security event log. To ensure that you can monitor your network security, enable Windows security auditing on all computers in your network.

- Identify computer drives formatted with the FAT32 file system

  The FAT32 file system offers little to no security. NTFS provides the ability to assign permissions to files and folders, thus controlling access to the resources.

Resource Objects

Windows XP Professional, Windows 2000, or Windows NT computers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event for successful discovery? (y/n)	Set to **y** to raise an event if discovery completes successfully. The default is n.
Event severity when discovery...	Set the event severity level, from 1 through 40, to indicate the importance of the event when discovery: **...succeeds**. The default is 25 (blue event indicator). **...fails**. The default is 5 (red event indicator). **...is partially done**. The Knowledge Script returns some data but also generates warning messages. The default is 10 (red event indicator). **...is not applicable**. This type of failure usually occurs when the target computer does not have Microsoft Windows Security installed.The default is 15 (yellow event indicator).
Check Security Log for default settings	Set to **y** to check the security log for default settings. The default is y.

Handling Events

Events raised by this Knowledge Script indicate inadequate Security log settings, disabled auditing, or the presence of the File Allocation Table (FAT) and FAT32 file system.

If the Security log is not set to overwrite events, this log may fill quickly, causing you to miss possible important events. Enable this setting or instill procedures to clean up the log.

If the Security log is set with a maximum capacity of 512KB, consider increasing the log capacity. In many environments, 20MB is adequate.

If computers are discovered using the FAT or FAT32 file system, consider converting all such drives to the NT File System (NTFS).

FAT and FAT32 file systems are simple, interoperable, and easy to restore, but they do not provide any security. In contrast, NTFS provides the ability to assign permission to files and folders, thus controlling who has access to the resources.

If inadequate auditing is enabled, enable auditing. The following table shows the required minimum auditing level for monitored Windows NT computers:

Event category	Audit level
Logon and Logoff	Success, Failure
Restart, Shutdown, and System	Success
Security Policy Changes	Success
User and Group Management	Success, Failure

The following table shows the required minimum auditing level for monitored Windows 2000 and Windows XP Professional computers:

Event category	Audit level
Audit account management	Success, Failure
Audit logon events	Success, Failure
Audit policy change	Success
Audit system events	Success

SharePoint

Use this Knowledge Script to discover configuration and resource information for Sharepoint servers. Discovery_SharePoint also tracks, displays, and provides various alerts about SharePoint services.

If you are running Microsoft SharePoint on multiple servers as part of your server farm, run Discovery_SharePoint on each server in the farm. In the Operator Console, each server from the farm displays individually in the TreeView, not as a group.

To ensure the functionality of SharePoint Knowledge Scripts, enable SharePoint logging so that log files are created. For more information, see the Microsoft SharePoint documentation.

Resource Objects

SharePoint servers

Default Schedule

By default, this script runs **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event when the discovery succeeds?	Select **Yes** to raise an event if this script successfully discovers SharePoint resources. The default is unselected.
Event severity when the discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance when this script successfully discovers SharePoint resources. The default is 25.
Raise event when the discovery fails?	Select **Yes** to raise an event if this script does not successfully discover SharePoint resources. The default is Yes.
Event severity when the discovery fails	Set the event severity level, from 1 to 40, to reflect the importance when the script fails to discover SharePoint resources. The default is 5.
Raise event when the discovery partially succeeds?	Select **Yes** to raise an event if this script only partially discovers SharePoint resources. The default is Yes.
Event severity when the discovery partially succeeds?	Set the event severity level, from 1 to 40, to reflect the importance when the script only partially discovers SharePoint resources. The default is 10.

SharePoint2010

Use the Discovery_SharePoint2010 Knowledge Script to discover configuration and resource information for SharePoint 2010 Servers. The Discovery script also tracks, displays, and provides various alerts about SharePoint services.

Note
After you discover SharePoint 2010 resources, two SharePoint tabs will display in the Knowledge Scripts pane: SHAREPOINT and SHAREPOINT2010. Run all SharePoint Knowledge Scripts from the SHAREPOINT2010 tab.

If you are running Microsoft SharePoint 2010 on multiple servers as part of your server farm, run Discovery_SharePoint2010 on each server in the farm. In the Operator Console, each server from the farm displays individually in the TreeView, not as a group.

By default, this script runs once for each computer.

Tip
Run this script on a scheduled basis to discover new SharePoint resources, such as Web applications.

Set the Values tab parameters as needed.

Description	How to Set It
Raise event when the discovery succeeds?	Select **Yes** to raise an event if this script successfully discovers SharePoint resources. The default is unselected.
Event severity when the discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance when this script successfully discovers SharePoint resources. The default is 25.
Raise event when the discovery fails?	Select **Yes** to raise an event if this script does not successfully discover SharePoint resources. The default is Yes.
Event severity when the discovery fails	Set the event severity level, from 1 to 40, to reflect the importance when the script fails to discover SharePoint resources. The default is 5.
Raise event when the discovery partially succeeds?	Select **Yes** to raise an event if this script only partially discovers SharePoint resources. The default is Yes.
Event severity when the discovery partially succeeds?	Set the event severity level, from 1 to 40, to reflect the importance when the script only partially discovers SharePoint resources. The default is 10.

Siebel

Use this Knowledge Script to discover Siebel eBusiness Application components on Windows computers. This Knowledge Script discovers Siebel Servers, Siebel Gateways, Siebel Web Extensions, and the Resonate Central Dispatch component.

Prerequisite

Add the computer with Siebel components to the Operator Console TreeView and store the Siebel Administrator user name and password in the AppManager repository with Security Manager.

The Administrator user name and password are required to start the `srvrmgr` command line utility.

Complete the following fields in the Custom tab of Security Manager for the Siebel computer.

Field	Description
Label	`SiebelUser`
Sub-label	`SiebelUser`
Value 1	Valid Siebel Administrator username to use on the selected computer.
Value 2	Password associated with the username you provided in the **Value 1** field.
Extended application support	Required field. Encrypts the username and password in Security Manager.

Resource Objects

Any Windows computer with a Siebel eBusiness Application component installed.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Siebel enterprise name	Set the Siebel enterprise name.
Siebel enterprise gateway name	Set the hostname of the Siebel gateway.
Siebel language	Select the language. You can choose one of the languages that is supported with your version of Siebel. The default is English (United States).
Siebel Server in Cluster Group	Select this checkbox if you have Siebel Servers in a cluster.
Siebel Server virtual host name	Set the virtual host name of the Siebel Server in a cluster.

Parameter	How to Set It
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **... succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **... fails**. The default is 5 (red event indicator). • **... is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages (for example, because AppManager for Siebel service could not be started, restarted, or it does not exist on the target computer). The default is 15 (yellow event indicator).

Siemens

Use this Knowledge Script to discover the resource and configuration information for Siemens PRIMERGY servers running Siemens ServerView. This Knowledge Script requires SNMP to be running on the computer you are discovering. If a required service is not found or is not running, the Discovery job fails with a "Not a Siemens Server" event.

Note
Because SNMP is not installed on Siemens servers by default, you may need to install it and restart the server before you can run this Knowledge Script successfully.

Resource Objects

Siemens servers

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
SNMP community string	Enter the SNMP community name to use. The default is the community name entered in the AppManager Security Manager or public if no community name has been entered.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...partially succeeds**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have Siemens ServerView installed. The default is 15 (yellow event indicator). **Note** If required services, such as SNMP, aren't running on the computer you are discovering, you may see a severity 15 event (Not a Siemens Server). If you see this type of event, see the detail message for more information about what caused the discovery to fail.

SNA

Use this Knowledge Script to discover Microsoft SNA Server configuration and resources.

Resource Objects

SNA server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have SNA Server installed. The default is 15 (yellow event indicator).

Snmp

Use this Knowledge Script to discover SNMP-enabled devices running on a network. The AppManager agent on which AppManager for SNMP is installed acts as a proxy for discovering SNMP devices. This AppManager agent is referred to as the SNMP proxy agent.

AppManager for SNMP supports SNMP versions 1, 2, and 3. If you do not specify an SNMP version, then AppManager will attempt to determine the version during the Discovery job. This process could be quite time consuming.

In a successful discovery, the following details are discovered:

Object	Discovered Details
SNMP Proxy object	Agent Address – The hostname or IP address of the SNMP proxy agent.
SNMP Device object	• Device Address — The hostname or IP address under which the device was discovered. • SNMP Version – The SNMP version being used by the SNMP device. • System Name – The value of the SNMP attribute `sysName.0`. • Vendor – The name of the vendor that manufactured the device. • OID – System OID from `sysObjectID.0` that uniquely identifies the type of device. • Services – The network services supported by the device, as specified by `sysServices.0`. • Contact – The value of `sysContact.0`. • Location – The value of `sysLocation.0`.

Devices can only be discovered by providing a device list of hostnames, IP addresses or IP address ranges for the corresponding Discovery Knowledge Script parameters. There is no automatic discovery capability. The Discovery_Snmp script iteratively attempts to contact and retrieve the System MIB from each supplied hostname or IP address.

Because many SNMP devices (typically routers) have multiple IP addresses, some devices may be discovered multiple times. In these cases, the Discovery script automatically detects and removes the duplicates from the list of discovered devices. Any duplicates are shown in the AppManager TreeView pane under the IP address or hostname under which they were first discovered.

During discovery, various errors may occur with the supplied list of SNMP devices. Most commonly, these will be SNMP timeouts from devices failing to respond because they are down, because they are not running an SNMP agent, or because the community string supplied for the device is incorrect. Other common errors can be due to bad hostnames or SNMP Response errors.

Discovery can take anywhere from a few seconds to several minutes or hours. The time taken largely depends on how many SNMP timeouts occur. For example, if this script is configured with an **SNMP timeout** value of 5 seconds and 3 **SNMP retries**, it takes 20 seconds to determine that the device is not responding.

You can control the time it takes discovery to finish by limiting the use of IP address ranges, which are likely to contain many addresses that are not used or that do not correspond to SNMP devices, and to keep the SNMP timeout/retry values as small as is practical for the local network environment.

Prerequisite

Before using this script, configure AppManager Security Manager with the community string and version information for each device you want to discover.

The type of information you configure varies according to the version of SNMP implemented on the device. AppManager for SNMP supports SNMP versions 1, 2, and 3.

Configuring SNMP information allows AppManager to access the MIBs on SNMP-enabled devices.

If you do not explicitly configure SNMP information for AppManaager for SNMP, the Snmp Knowledge Scripts can search for and use community strings you may have already configured for use by the AppManager for Network Device module.

Configuration for SNMP Versions 1 and 2

Configure community string and version information for each device monitored by each proxy computer.

Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`SNMP`
Sub-label	Indicates whether the user name and context you are configuring will be used for a single device or for all devices. • *For a single device* on a particular proxy agent computer, enter *<device name>*. • *For all devices* on a particular proxy agent computer, enter `default`.
Value 1	The appropriate read-only community string value, such as `private` or `public`.
Value 3	• `v1` or `1` if the device supports SNMPv1. • `v2` or `2` if the device supports SNMPv2. If you do not specify either SNMP version, AppManager attempts to determine the version during the Discovery job. This process can be quite time consuming.

Configuration for SNMP Version 3

AppManager for SNMP supports the following modes for SNMP version 3 (SNMPv3):

- No authentication; no privacy
- Authentication; no privacy
- Authentication and privacy

In addition, the module supports the following protocols for SNMPv3:

- MD5 (Message-Digest algorithm 5, an authentication protocol)
- SHA (Secure Hash Algorithm, an authentication protocol)
- DES (Data Encryption Standard, encryption protocol)

Your SNMPv3 implementation may support one or more combinations of mode and protocol. That combination dictates the type of information you configure in AppManager Security Manager: user name (or entity), context name, protocol name, and protocol passwords.

You need to configure SNMPv3 information for each device monitored by each proxy computer.

Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	`SNMP`

Field	Description
Sub-label	Indicates whether the user name and context you are configuring will be used for a single device or for all devices. • *For a single device* on a particular proxy agent computer, enter <*device name*>. • *For all devices* on a particular proxy agent computer, enter `default`.
Value 1	The appropriate read-only community string value, such as `private` or `public`. All SNMPv3 modes require an entry in the **Value 1** field.
Value 2	The name of a context associated with the user name or entity you entered in the Value 1 field. A context is a collection of SNMP information that is accessible by an entity. If possible, enter a context that provides access to all MIBS for a device. If the device does not support context, type an asterisk (*). All SNMPv3 modes require an entry in the **Value 2** field.
Value 3	The combination of protocol and password appropriate for the SNMPv3 mode you have implemented. • For *no authentication/no privacy mode*, leave the **Value 3** field blank. • For *authentication/no privacy mode*, enter `md5` or `sha` and the password for the protocol, separating each entry with a comma. For example, enter `md5,abcdef` • For *authentication/privacy mode*, enter `md5` or `sha` and the associated password, and then enter `des` and the associated password, separating each entry with a comma. For example, enter `sha,hijklm,des,nopqrs`

Resource Objects

NT_MachineFolder

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Discovery Parameters	
List of SNMP devices	Supply a list of SNMP device hostnames or IP addresses. An attempt is made to discover each device listed. The default is `localhost`. **Note** The SNMP information for each device you list in this field must be entered into Security Manager before you can run this script.
Address ranges of SNMP devices	Supply a list of IP address ranges. Each range must be in the format "`A.B.C.D-W.X.Y.Z`". For example, enter "`10.1.1.0-10.1.1.254`". Each address range may be no longer than 255 addresses, although they can span subnets. For example, "`10.1.1.250-10.1.2.30`" spans a subnet. The default is blank. **Note** The SNMP information for each device in a range must be entered into Security Manager before you can run this script.

Parameter	How to Set It
Full path to file with list of SNMP devices	Supply the full path to a file containing a list of individual IP addresses or hostnames. The file path supplied must be accessible from the SNMP proxy agent, not the AppManager Operator Console or repository computer. Device names may be separated by commas, blank characters or new lines. The default is blank. **Note** The SNMP information for each device listed in the file must be entered into Security Manager before you can run this script.
Maximum number of devices to discover	Specify the maximum number of devices to be discovered. Discovery stops when this limit is reached, even if not all IP addresses and hostnames have been attempted. The default and maximum allowed value is 50.
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default is `161`.
SNMP retries	Specify the number of retries to attempt if a timeout occurs on an SNMP request. The default is 1 retry.
SNMP timeout	Specify the number of seconds to wait for a response before timing out an SNMP request. The default is 3 seconds.
Trap Receiver Discovery	
Discover Trap Receiver?	Set to **Yes** to discover NetIQ SNMP Trap Receiver. The default is Yes.
Trap Receiver IP address	Specify the IP address of the computer on which Trap Receiver is installed. The default is `localhost`.
Trap Receiver TCP port	Specify the TCP port number through which Trap Receiver will communicate with AppManager. The default is port 2735.
Event Notification	
Raise event if discovery succeeds?	Set to **Yes** to raise an event if discovery is completely successful. The details of the event contain the list of discovered devices.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25. Discovery is successful if all devices in the device list are discovered and no errors occur. The event message indicates any duplicate IP addresses or hostnames. Duplicates are not considered to be an error.
Raise event if discovery partially succeeds?	Set to **Yes** to raise an event if discovery is partially successful. The details of the event contain the list of discovered devices and the discovery errors that occurred.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery partially succeeds. The default is 15. A partial discovery occurs if only some of the SNMP devices are discovered, or if the maximum device limit is reached. The event message indicates any duplicate IP addresses or hostnames. Duplicates are not considered errors.
Raise event if discovery fails?	Set to **Yes** to raise an event if no SNMP devices are discovered. The details of the event contain the discovery errors that occurred.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no SNMP devices are discovered. The default is 10.

SQL

Use this Knowledge Script to discover Microsoft SQL Server configuration and resources.

Note
In order to successfully discover a SQL Server instance, that instance must be running when you run the Discovery Knowledge Script.

Resource Objects

SQL Server computer.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
User name	Enter the username for the account used to log on to the SQL Server(s) you want to discover. In order to perform a complete discovery of SQL Server components, use an account that is assigned to the role of System Administrator for each SQL Server. Accounts assigned to SQL Server roles with fewer permissions are not able to discover all components. The default is the sa user account.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have a SQL Server installed. The default is 15 (yellow event indicator).

SQL-RT

Use this Knowledge Script to discover if AppManager ResponseTime for SQL components are available on a specific managed client. At the Operator Console, run this Knowledge Script on the managed client on which you are performing discovery.

After successful discovery, a new thumbnail appears in the TreeView pane with a list of computers on which you are performing discovery.

Resource Objects

Windows XP Professional, Windows 2000, or Windows NT.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can select the **Yes** check box to raise an event when the job succeeds. By default, events are not raised on success.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. This type of failure usually occurs when the target computer does not have all the prerequisites installed. The default is 10 (red event indicator).

StreamingMedia-RT

Use this Knowledge Script to discover the StreamingMedia-RT managed object on a resource in the TreeView pane of the Operator Console.

Resource Objects

Any Windows XP Professional, Windows Server 2003, Windows 2000 Server, or Windows NT Server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the **Values** tab parameters as needed.

Parameter	How to Set It
Event for successful discovery?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds.
Event severity when discovery succeeds	Set the severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery is partially done	Set the severity level, from 1 to 40, to reflect the importance of an event in which discovery returns some data but also generates warning messages. The default is 10.

UNIX

Use this Knowledge Script to discover NetIQ Corporation UNIX agents on managed UNIX servers. This Knowledge Script can discover configuration and resource information for many types of UNIX operating environments and servers, including Sun Solaris, Red Hat Linux, SuSE Linux, HP-UX, and IBM AIX platforms.

Resource Objects

UNIX computer icon.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed::

Description	How to Set It
Raise event if discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to y to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25. • **...fails**. The default is 5. • **...is partially done**. This type of event usually indicates the operating environment on the target computer is not supported or not recognized. The default is 15.
Discover printers?	Set this parameter to y if you want discovery to include printer resources. By default, printers are discovered.

VirtualCenter

Use the Discovery_VirtualCenter Knowledge Script to discover VMware vCenter resources. Run the script on vCenter servers and agent computers that can monitor vCenter.

Performing a discovery of a large VMware deployment can be a resource-intensive process that might cause performance-related events in AppManager and console unresponsiveness until discovery is completed.

You can use the parameters under *Detailed object settings* to filter the number of resource objects and resource object details that are discovered, such as CPU, memory, network, and disk details. Filtering these objects will reduce the time and resources required for performing discovery. However, limiting the number of discovered objects also limits the Knowledge Script jobs you can run.

For example, if you disable the *Discover datastores?* parameter, you cannot run the DataStoreUsage Knowledge Script, because no datastore objects get discovered. Similarly, if you run the VirtualMachineInventory Knowledge Script, it prompts a re-discovery that will bypass the discovery of datastores, again because no datastore objects get discovered.

Note
This module does not support the use of a pipe character ("|") in the name of a virtual machine, host, cluster, datastore, resource pool, or other resource object. If a pipe character is present in a resource object name, such as `Test|machine`, the VMware Knowledge Scripts will not be able to monitor that object, nor will the scripts be able to monitor a collection of virtual machines containing that resource object.

You can also the Discovery_VirtualCenter script to create exclusions lists for hosts and virtual machines (VMs) for hosts and VMs you do not with to display in the AppManager for VMware TreeView.

Resource Objects

vCenter servers and agent computers that can monitor VMware vCenter

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity if Discovery job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Discovery job fails unexpectedly. The default is 5.
Additional Settings	
Event Details	
Event detail format	Select either **HTML Table** or **Plain Text** as the format for event detail. The default is HTML Table.

Description	How to Set It
Raise event if Discovery succeeds?	Select **Yes** to raise an event if discovery succeeds in finding VMware vCenter resources. The default is Yes.
Event severity if Discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds in finding VMware vCenter resources. The default is 25.
Raise event if excluded objects were not found?	Select Yes to raise an event if the objects you listed in the *Hosts to exclude* and the *Virtual machines to exclude* parameters were not found during the discovery process. The default is Yes.
Event severity if excluded objects not found?	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the objects you listed in the exclusion list were not found during the discovery process. The default is 15.
Raise event if Discovery fails?	Select **Yes** to raise an event if discovery fails to find VMware vCenter resources. The default is Yes.
Event severity if Discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery fails to find VMware resources. The default is 5.
Discover vCenter	
Detailed object settings	
Discover datastores?	Select **Yes** to discover datastore objects. Disable this parameter to reduce the number of objects that are discovered. The default is Yes. **Note** If you disable this parameter, you cannot run the DataStoreUsage Knowledge Script because no datastore objects are discovered.
Discover cluster details?	Select **Yes** to discover cluster details. Disable this parameter to reduce the number of resource object details that are discovered. The default is Yes.
Discover resource pool details?	Select **Yes** to discover resource pool details. Disable this parameter to reduce the number of resource object details that are discovered. The default is Yes.
Discover hosts?	Select **Yes** to discover hosts. Disable this parameter to reduce the number of resource object details that are discovered. The default is Yes.
Discover host details?	Select **Yes** to discover host details. Disable this parameter to reduce the number of resource object details that are discovered. The default is Yes.
Hosts to exclude (comma separated)	List any hosts you do not with to display in the AppManager for VMware TreeView. Separate the host names with commas and without spaces. Creating an exclusion list like this can prove useful if you have two hosts co-located underneath a single vCenter server. A single VMware module discovery will discover both hosts, and this module will monitor them together as one environment. As a result, you cannot use monitoring policies on just one of the hosts unless you list the host or hosts you want to exclude.
Full path to file containing list of hosts to exclude	Provide the path to a location on the agent computer that contains the file with the list of hosts you want to exclude.
Discover virtual appliances?	Select **Yes** to discover pre-built software solutions called virtual appliances, or vApps. Disable this parameter to reduce the number of resource object details that are discovered. The default is Yes.

Description	How to Set It
Discover virtual appliance details?	Select **Yes** to discover virtual appliance details. Disable this parameter to reduce the number of resource object details that are discovered. The default is Yes.
Discover virtual machines?	Select **Yes** to discover virtual machine objects. Disable this parameter to reduce the number of objects that are discovered. The default is Yes. **Note** If you disable this parameter, you cannot run the following Knowledge Scripts, because no virtual machine objects are discovered: • VmConnected • VmCPUUsage • VmDiskIO • VmDiskUsage • VmMemoryUsage • VmNetworkIO • VmPowerStatus • VmToolsStatus
Discover virtual machine details?	Select **Yes** to discover virtual machine details. Disable this parameter to reduce the number of resource object details that are discovered. The default is unselected. **Note** To discover virtual machine details, you must also select **Yes** for *Discover virtual machines?*
Discover virtual machine templates?	Select **Yes** to discover virtual machine templates. The default is unselected. If you do not select Yes, templates are not discovered and are treated as if they were functional virtual machines. **Note** To discover virtual machine templates, you must also select **Yes** for *Discover virtual machines?*
Virtual machines to exclude (comma separated)	List any virtual machines you do not with to display in the AppManager for VMware TreeView. Separate the names with commas and without spaces. Creating an exclusion list like this can prove useful if you have two virtual machines co-located underneath a single vCenter server. A single VMware module discovery will discover both entities, and this module will monitor them together as one environment. As a result, you cannot use monitoring policies on just one of the virtual machines unless you list the virtual machine or machines you want to exclude.
Full path to file containing list of virtual machines to exclude	Provide the path to a location on the agent computer that contains the file with the list of virtual machines you want to exclude.

VoIPQuality_CallPerf

Use this Knowledge Script to discover the VoIP Quality-Call Performance managed object on a resource in the TreeView pane of the Operator Console.

Resource Objects

Any Windows XP Professional, Windows Server 2003, Windows 2000 Server, or Windows NT Server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the **Values** tab parameters as needed.

Parameter	How to Set It
Event for successful discovery?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery is partially done	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery returns some data but also generates warning messages.

VoIPQuality_CallPerfProxy

Use this Knowledge Script to discover a Call Performance computer that does not have the AppManager agent installed but does have the NetIQ Performance Endpoint installed. Discovery is successful *only* if the managed object is able to communicate with the endpoint on the target computer. With successful discovery, the CallPerf Proxy object is created in the TreeView pane.

Note
You should only have one computer acting as a proxy for a given remote computer. Therefore, you may drop this script on only one computer at a time.

Resource Objects

Any Windows XP Professional, Windows Server 2003, Windows 2000 Server, or Windows NT Server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the **Values** tab parameters as necessary.

Parameter	How to Set It
List of remote computers	Enter a list of the remote computers for which you want to discover Call Performance resources. You must specify at lease one remote computer. Use a comma to separate the names in the list: `raldbellijm02,raldattixlm`
Full path to file with list of computers	Instead of listing each remote computer separately, you can specify the full path to a file on the agent computer that contains a computer name on each line of the file.
Event for successful discovery?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.

VoIPQuality_CallSetup_H.323

Use this Knowledge Script to discover configuration information and resources for the H.323 protocol.

Resource Objects

Windows XP Professional, Windows Server 2003, Windows 2000 Server, or Windows NT Server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the **Values** tab parameters as needed.

Parameter	How to Set It
Event for successful discovery?	This script always raises an event when the discovery fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.

VoIPQuality_CallSetup_SIP

Use this Knowledge Script to discover the SIP (Session Initiation Protocol) managed object in the TreeView pane of the Operator Console.

Resource Objects

Any Windows XP Professional, Windows Server 2003, Windows 2000 Server, or Windows NT Server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the **Values** tab parameters as needed.

Parameter	How to Set It
Event for successful discovery?	This script always raises an event when the discovery fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.

VoIPQuality_CiscoSAA

Use this Knowledge Script to discover a computer on which the Cisco SAA software is installed. You run this script on the computer that will be used as the proxy, or owner, for all of the routers on which the CiscoSAA software is installed. Because you should only have one computer acting as a proxy for any given set of routers, run this script on only one computer at a time.

Discovery is successful *only* if the managed object is able to communicate with the Cisco router on the target computer. If the discovery is successful, the Cisco SAA object is created in the TreeView pane.

Configuring Community String Information for Cisco SAA

If your community string information is the same for all Cisco SAA routers, complete the following procedure once. If your community string information is different for different routers, complete the following procedure once for each different community string.

You must update Security Manager before you can discover Cisco SAA resources.

Complete the following fields in the Custom tab of Security Manager for the proxy agent computer.

Field	Description
Label	SAA
Sub-label	Indicates whether the community string information will be used for a single router or for all routers. • *For a single router*, enter <*`router name`*>. • *For all routers using the selected computer as proxy*, enter <*`computer name`*>. • For all routers, enter `default`.
Value 1	Appropriate read/write community string value, such as `private` or `public`.

Resource Objects

Any Windows XP Professional, Windows Server 2003, Windows 2000 Server, or Windows NT Server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
List of remote computers	Enter a list of the remote computers for which you want to discover Cisco SAA resources. You must specify at least one remote computer. Use a comma to separate the names in the list: `raldbellijm02,raldattixlm`
Full path to file with list of computers	Instead of listing each remote computer separately, you can specify the full path to a file on the agent computer that contains a computer name on each line of the file. **Note** The community string information for each of the computers that you list in this field must be entered into Security Manager before you can run this script.
Event for successful discovery?	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.

Web-RT

Use this Knowledge Script to discover AppManager ResponseTime for Web resources.

The discovery Knowledge Script looks for the Web-RT managed object that monitors Web sites, services, Web transactions, and related protocols.

An event is always raised if the job fails. You can also enable events to notify you when discovery succeeds or is partially successful (that is, discovers some resources but also generates errors).

Resource Objects

Windows XP Professional, Windows 2000, Windows NT, and Windows Server 2003.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can select the **Yes** check box to raise an event when the job succeeds. By default, events are not raised on success.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...partially succeeds**. This type of failure usually occurs when the target computer does not have all the prerequisites installed. The default is 10 (red event indicator).

WebLogicSvr

Use this Knowledge Script to discover WebLogic Server installed on Windows servers. This Knowledge Script returns information about successful, failed and partial discoveries and raises events (with user-specified severity) to notify you of errors.

This Knowledge Script may be used to determine if and where WebLogic Servers are installed in a Windows network. It is useful to run this Knowledge Script periodically to detect new instances of WebLogic Servers and to determine if existing servers have been uninstalled or taken offline.

For other Knowledge Scripts to gather the information they need, this Knowledge Script starts agents that can provide the information. One NetIQ WebLogic agent is started for each release of WebLogic that is discovered on the machine. For example, if releases 6.1 and 7.0 are both installed on the same machine, one NetIQ WebLogic agent will be started for release 6.1 and one NetIQ WebLogic agent will be started for release 7.0.

These agents can be disabled (and enabled) via the WebLogicSvr_NetIQAgent Knowledge Script.

Resource Objects

WebLogic Server, versions 6.0, 6.1, 7.0, and 8.1.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	Set to **y** to raise an event when the Knowledge Script discovers a WebLogic Server. The default is y.
Event severity when Discovery succeeds	Specify a severity level for the event raised by successful discovery of a WebLogic Server. The default is 25.
Event severity when Discovery fails	Specify a severity level for the event raised by failure to discover a WebLogic Server. The default is 5.
Event severity when Discovery is partially done	Specify a severity level for the event raised when the Knowledge Script starts but does not run to completion. The default is 10.
Administration Server hostname:port. Must match Security Manager entry.	Specify the hostname containing an Administration Server for the WebLogic domain and the port number on which the Administration Server is listening. The hostname and port must be separated by a colon. This should match the entry in the Security Manager. If you want to discover multiple servers during discovery and need to contact more than one Administration Server, multiple hostname/port combinations can be specified. Multiple hostname/port combinations will be separated by semi-colons. Ensure all combinations have been entered into Security Manager. For example: `localhost:80;storm:888;wilder:1333` The default is `localhost:7001`.

BEA home directory. Must contain the BEA `registry.xml` file.	Specify the home directory of your WebLogic Server installation. This directory should contain the `registry.xml` file. If you want to discover multiple installations of WebLogic during discovery, multiple directories can be specified. Multiple directories will be separated by semi-colons. For example: `c:\bea70;c:\bea81.` The default is `c:\bea`.
Directory in which to search for a Java Runtime Environment.	Specify a directory in which a Java Runtime Environment is installed. A 1.3 JRE or greater is required. A 1.4 JRE is required for WebLogic Server 8.1. Note that there is no default.
Port to use for NetIQ Web Logic Server agent.	Specify the port on which the NetIQ WebLogic agent receives requests. If multiple versions of WebLogic are to be discovered, each version will require a unique port. Multiple ports must be separated by semi-colons. For example: 2000;2001. The default is 2000.

WebLogicSvrUNIX

Before you run this Knowledge Script, you must update the AppManager repository with the WebLogic Server administrator account information for the server you want to discover.

Use this Knowledge Script to discover WebLogic Server installed on UNIX servers. This script returns information about successful, failed and partial discoveries and raises events (with user-specified severity) to notify you of errors.

This script is used to determine if and where WebLogic Servers are installed in a UNIX network. It is useful to run this script periodically to detect new instances of WebLogic Servers and to determine if existing servers have been uninstalled or taken offline.

To allow other Knowledge Scripts to gather the information they need, this script starts agents that can provide the information. One NetIQ WebLogic agent is started for each release of WebLogic that is discovered on the computer.

These agents can be disabled (and enabled) via the WebLogicSvrUNIX_NetIQAgent script.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **only once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event when discovery succeeds? (y/n)	Set to **y** to raise an event when the Knowledge Script discovers a WebLogic Server. The default is y.
Event severity when discovery succeeds	Specify a severity level for the event raised by successful discovery of a WebLogic Server. The default is 25.
Event severity when discovery fails	Specify a severity level for the event raised by failure to discover a WebLogic Server. The default is 5.
Event severity when discovery partially succeeds	Specify a severity level for the event raised when the Knowledge Script starts but does not run to completion. The default is 10.
Communication Channel (Clear Text/ SSL)	Select the channel for communication with a WebLogic Server. The default communication channel is Clear Text. **Note** The SSL option is available only for WebLogic Server versions 9.x and 10.x.
Trusted Server CA Certificate (applicable if communication channel is SSL)	Specify the path for the trusted server CA certificate. **Note** Specify the certificate path only if you select SSL for the **Communication Channel** parameter.

Administration Server hostname:port. Must match Security Manager entry	Specify the hostname containing an Administration Server for the WebLogic domain and the port number on which the Administration Server is listening. The hostname and port must be separated by a colon. If you are discovering multiple servers and need to contact more than one Administration Server, specify each hostname:port combination, separated by a semi-colon. Do not add spaces before or after the semicolon. For example: `localhost:80;storm:888;wilder:1333` The default is `localhost:7001`. **Note** Ensure that all combinations are entered in Security Manager.
BEA home directory. Must contain the BEA registry.xml file	Specify the home directory of your WebLogic Server installation. This directory should contain the `registry.xml` file. If you are discovering multiple installations of WebLogic, specify each home directory, separated by a semi-colon. Do not add spaces before or after the semicolon. For example: `/usr/weblogic;/opt/web/weblogic` The default is `/usr/`.
Directory to search for a Java Runtime Environment	Specify a directory in which a Java Runtime Environment is installed. Note that there is no default.
Port to use for NetIQ WebLogic Server agent.	Specify the port on which the NetIQ WebLogic agent receives requests. If you are discovering multiple versions of WebLogic, specify each version with a unique port, separated by semi-colons. For example: `2000;2001`. The default is 2000.

WebServices

Use this Knowledge Script to discover the NetIQ AppManager Web Services managed object that monitors Web sites, services, and related protocols.

Resource Objects

Web Services.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have the Web Services agent installed. The default is 15 (yellow event indicator).

WebSphereAppSrv

Use this Knowledge Script to discover instances of the WebSphere Application Server. The Discovery Knowledge Script can be used to discover any or all of the application servers running on a computer. However, if multiple application servers (associated with either a single WebSphere installation, or multiple coexisting installations) are to be discovered on a single computer, they must all be discovered simultaneously, with a single execution of the Discovery script. This is because each time discovery is run, the discovered objects replace any existing discovered resources in the TreeView, so that if one instance is discovered and then a second instance is discovered, the resources associated with the instance discovered first will be lost.

For resources to be successfully discovered, each of the following requirements must be met. If any of these requirements are not met, discovery fails:

- The perfservlet Web application must be deployed and running on a server in the WebSphere domain. (The computer on which the perfservlet is deployed need not be the same as the computer being discovered, but it must be in the same WebSphere domain.) The perfservlet is included with WebSphere, and can be found in the `installableApps` directory. You will need to deploy the servlet and start it running before you can successfully execute this Discovery script. The perfservlet can be deployed easily by accepting all defaults when using the application deployment wizard.
- The perfservlet must be able to retrieve performance data for the application server(s) running on the node(s) being discovered. This implies that the application servers are running, and that performance monitoring has been enabled on the application servers. To discover all WebSphere resources, the monitoring levels for all modules should be set to High. (If you want to run most of the JVM Runtime Knowledge Scripts, the JVM Runtime monitoring levels should be set to Maximum, and the `-XrunpmiJvmpiProfiler` switch should be included as an argument to the Application Server JVM process.)
- The WebSphere installation must be found in one of the directories specified as a parameter to this script. You can specify the `WebSphere\AppServer` directory, or the `WebSphere` directory.

The Discovery script returns information about components of the WebSphere Application Server, such as the EJBs that are deployed on the server, the JDBC providers and data sources, installed Web applications and servlets, as well as other components. If new applications are deployed to the server, or other changes are made to the configuration of application server components, the Discovery Knowledge Script should be run again to pick up the changes. It is strongly recommended that the existing WebSphere Server resource object be deleted from the Operator Console TreeView before Discovery is performed again.

This Knowledge Script takes as a parameter the URL of the perfservlet Web application. This URL is relative to the computer being discovered, so the default URL, which points to `localhost`, will probably work on most single-host WebSphere deployments. However, in multi-node WebSphere deployments, the perfservlet normally runs on a single server in the domain. In such cases, you will need to change the value of this parameter to point to the proper location.

It is possible to run discovery against multiple computers at once, by dropping the Discovery script on a server group. However, all application servers being discovered concurrently must be members of the same WebSphere domain, with the same perfservlet URL providing performance data for each of the servers. If you run the Discovery script against more than one server, make sure you change the URL from `localhost` to the appropriate hostname, or each server will attempt to contact the perfservlet on the local computer.

If it is necessary to go through a proxy server to access the perfservlet URL, you will need to specify the proxy server (hostname or IP address) and the proxy server port number. In addition, if the proxy server requires a login and password, you will need to supply them here. If no proxy lies between the agent computer and the perfservlet, you can leave all four proxy fields blank.

Note
If you specify a proxy server, the perfservlet URL that you specify should not include a hostname of "localhost", because localhost will be interpreted by the proxy server, causing the proxy server to attempt to connect to itself. When using a proxy server, the perfservlet URL must specify the actual hostname of the computer being discovered.

If you specify a proxy server, it will be used when accessing the optional servlet URL specified in the HealthCheck Knowledge Script, as well as when accessing the perfservlet. You cannot specify a separate proxy, or no proxy, for the HealthCheck servlet.

As part of the discovery process, this Knowledge Script starts a persistent agent running on the discovered host. This agent must be running in order for most of the Knowledge Scripts to function. You must specify the port number where the agent should listen for requests. If you intend to run the RequestMetrics Knowledge Script, you must ensure that the same port number is specified for all the computers you discover. If you do not intend to use the RequestMetrics Knowledge Script, this restriction does not apply. However, you still must supply a valid (otherwise unused) TCP port number.

Versions of WebSphere Supported

4.0.2, 4.0.3, 4.0.4, 4.0.5, 4.1, 5.0, 5.0.1, 5.0.2

Resource Object

Windows Computer

Default Schedule

By default, this script is only run **once** per computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if discovery succeeds? (y/n)	Set to **y** to raise an event when the Knowledge Script discovers a WebSphere Application Server. The default is n.
Event severity when discovery succeeds	Specify the severity level, from 1 to 40, to indicate the importance of the event raised by successful discovery of a WebSphere Application Server. The default is 35.
Event severity when discovery fails	Specify a severity level, from 1 to 40, to indicate the importance of the event raised by failure to discover a WebSphere Application Server. The default is 5.

Perfservlet URLs (semicolon-separated)	Specify one or more URLs of the perfservlet Web application. (Multiple URLs are normally needed only if both WebSphere 4 and WebSphere 5 nodes need to be discovered on the target host.) For the discovery process to succeed, the perfservlet must be running and able to provide performance data for application servers running on the target host. Separate multiple URLs with semicolons (;).
Directories to search for WebSphere home directory (semicolon-separated)	Specify the list of directories to search for the WebSphere Application Server home directory. Separate multiple directories with semicolons (;).
TCP port for accepting requests	Specify the TCP port to be used by the agent when listening for requests. The same port must be specified for all computers on which the agent runs in order for the RequestMetrics Knowledge Script to function properly.
Proxy host	Specify the hostname or IP address of the machine on which the Web proxy server is running. Leave this field blank if no proxy server is in use.
Proxy port	Specify the port number to use when connecting to the proxy server. If you specify a proxy host, you must specify a port as well. If you are not using a proxy server, leave this field blank.
Proxy login	Specify the user name to use when logging into the proxy server. If the proxy server does not require authorization, or if a proxy server is not being used, leave this field blank.
Proxy password	Specify the password associated with the proxy login. If the proxy server does not require authentication, or if the login being used does not have an associated password, or if a proxy server is not being used, leave this field blank.

WebSphereAppSrvUNIX

Use this Knowledge Script to discover instances of IBM WebSphere Application Server.

Note
To discover EJB objects, you must have an application running EJB available when you run this Knowledge Script.

If a discovered IBM WebSphere Application Server object includes a colon (:) in the name, the Operator Console replaces the colon with a backslash (\). For example, if the object name is `Object: ws/WSSecureMap`, the object name is displayed as `Object\ ws/WSSecureMap`.

Use this script to discover any or all of the application servers running on a computer. However, if multiple application servers (associated with either a single WebSphere Application Server installation, or multiple coexisting installations) are to be discovered on a single computer, they must all be discovered simultaneously, with a single execution of the discovery script. This is because each time discovery is run, the discovered resources are replaced, so that if one instance is discovered, and then a second instance is discovered, the resources associated with the instance discovered first will be lost.

Before you discover IBM WebSphere Application Server, review the prerequisites to ensure that your environment is configured properly. For more information, see the *AppManager for IBM WebSphere Application Server UNIX Management Guide*.

This Knowledge Script takes as a parameter the URL of the Performance servlet Web application. This URL is relative to the computer being discovered, so the default URL, which points to localhost, will probably work on most single-host WebSphere Application Server deployments. However, in multi-node WebSphere Application Server deployments, the Performance servlet normally runs on a single server in the domain. In such cases, you will need to change the value of this parameter to point to the proper location.

It is possible to run discovery against multiple computers at once, by running the discovery script on a server group. However, all application servers being discovered concurrently must be members of the same IBM WebSphere Application Server domain, with the same Performance servlet URL providing performance data for each of the servers. If you run the discovery script against more than one server, make sure you change the URL from localhost to the appropriate hostname, or each server will attempt to contact the Performance servlet on the local computer.

If it is necessary to use a proxy server to access the Performance servlet URL, you need to specify the proxy server host name or IP address, and the proxy server port number. In addition, if the proxy server requires a login and password, you will need to supply them here. If no proxy lies between the agent computer and the Performance servlet, you can leave all four proxy fields blank.

Notes

- If you specify a proxy server, the Performance servlet URL that you specify should not include a hostname of localhost, because localhost will be interpreted by the proxy server, causing the proxy server to attempt to connect to itself. When using a proxy server, the Performance servlet URL must specify the actual hostname of the machine being discovered.
- The proxy server you specify will be used when accessing the optional servlet URL specified in the HealthCheck Knowledge Script, as well as when accessing the Performance servlet. You cannot specify a separate proxy, or no proxy, for the HealthCheck servlet.

As part of the discovery process, this Knowledge Script:

- Starts a Java server on the discovered host that the AppManager managed object uses to communicate with WebSphere Application Server.
- Specifies the port that the Java server uses to communicate with the managed object.

If you encounter problems with WebSphere Application Server Knowledge Scripts collecting performance data, use the NetIQAgent Knowledge Script to stop and restart the Java server.

If you intend to run the RequestMetrics *Knowledge Script,* you must ensure that the same port number is specified for all the computers you discover. If you do not intend to use the RequestMetrics Knowledge Script, this restriction does not apply. However, you still must supply a valid (otherwise unused) TCP port number.

Resource Object

UNIX Computer

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery? (y/n)	Set to **y** to raise an event when the script discovers IBM WebSphere Application Server. The default is n.
Event severity when Discovery succeeds	Specify a severity level for the event raised by successful discovery of IBM WebSphere Application Server. The default is 35.
Event severity when Discovery fails	Specify a severity level for the event raised by failure to discover IBM WebSphere Application Server. The default is 5.
Semicolon-separated list of perfservlet URLs	Specify one or more URLs of the Performance servlet Web application. Multiple URLs are normally needed only if both WebSphere 6.0 and WebSphere 6.1 nodes need to be discovered on the target host. For the discovery process to succeed, the Performance servlet must be running and able to provide performance data for application servers running on the target host.
Semicolon-separated list of directories to search for WebSphere home directory	Specify the list of directories to search for the WebSphere Application Server home directory.
TCP port for accepting requests	Specify the TCP port that the Java server uses to communicate with the AppManager managed object. The same port must be specified for all computers on which the agent runs in order for the RequestMetrics Knowledge Script to function properly. The default TCP port is 4000.
Proxy host	Specify the host name or IP address of the machine on which the Web proxy server is running. If you are not using a proxy server, leave this field blank.
Proxy port	Specify the port number to use when connecting to the proxy server. If you specify a proxy host, you must specify a port as well. If you are not using a proxy server, leave this field blank.

Proxy login	Specify the username to use when logging into the proxy server. If the proxy server does not require authorization, or if you are not using a proxy server, leave this field blank.
Proxy password	Specify the password associated with the proxy login. If the proxy server does not require authentication, or if the login being used does not have an associated password, or if you are not using a proxy server, leave this field blank.

WebSphereMQUNIX

Use this Knowledge Script to discover IBM WebSphere MQ (formerly **MQSeries**) Servers on UNIX, including WebSphere MQ Server queues, queue managers, and channels.

To successfully discover WebSphere MQ on UNIX, the `root` user must belong to the WebSphere MQ Server user group. Note that by default, the WebSphere MQ Server user group is **mqm**.

Resource Objects

WebSphere MQUNIX Server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Queue Managers Path	Enter the full path to the queue manager on the WebSphere MQ Server you want to discover. The default is: `/var/mqm/qmgrs`.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **... succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **... fails**. The default is 5 (red event indicator). • **... is partially done**. This type of failure usually occurs when the root user does not belong to the WebSphere MQ Server user group (by default this is **mqm**) or if there are multiple queues installed in different directories but one of the queues is not running. The default is 15 (yellow event indicator).

Win-RT

Use this Knowledge Script to discover settings for the Win-RT managed object and the Win-RT service. This script will also verify that a user domain, name, and password to be associated with the agent's Win-RT service have been entered in the AppManager Security Manager.

This script returns information about successful and failed discoveries and raises events (with user-specified severity) to notify you of errors.

Prerequisite

The domain, name, and password of the account to be associated with the ResponseTime for Windows service is stored in AppManager Security Manager. This information is be stored on a per-agent basis. An event is raised if no Security Manager entry is found for a given agent.

Complete the following fields in the Custom tab of Security Manager for the Windows agent computer.

Field	Description
Label	`Win-RT`
Sub-label	`ServiceAccount`
Value 1	Service account domain name
Value 2	Service account name
Value 3	Service account password
Extended application support	Required field. Encrypts the information in Security Manager.

Resource Object

NT_MachineFolder

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Specify a severity level for the event raised when an error prevents the script from completing. The default is 5.
Raise event with managed object trace results?	Set to **Yes** to raise an event containing the trace results from the managed object. Use the trace results for debugging purposes. The default is unchecked.
Event severity of managed object trace results?	Specify a severity level, from 1 to 40, to indicate the importance of an event raised with the trace results from the managed object. The default is 40.

Raise event if discovery successful?	Set to **Yes** to raise an event when the script discovers a Win-RT instance. The default is unchecked.
Event severity when discovery successful	Specify a severity level, from 1 to 40, to indicate the importance of an event in which the script discovers a Win-RT instance. The default is 25.
Raise event if discovery fails?	Set to **Yes** to raise an event when the script completes but does not discover a Win-RT instance. The default is checked (Yes).
Event severity when discovery fails	Specify a severity level, from 1 to 40, to indicate the importance of an event in which the script fails to discover a Win-RT instance. The default is 5.
Raise event if Win-RT managed object not installed?	Set to **Yes** to raise an event when the script completes but the Win-RT managed object is not found. The default is checked.
Event severity when Win-RT managed object not installed	Specify a severity level, from 1 to 40, to indicate the importance of an event in which the script determines the Win-RT managed object is not installed. The default is 5.

Win-RT7

Use this Knowledge Script to discover applications installed on systems with the Windows-RT managed object and the Windows-RT service. This script also verifies that the user domain, name, and password associated with the agent's Windows-RT service have been entered in AppManager Security Manager.

After you run the Discovery script on a server, any discovered applications display as individual objects under the Win-RT7 TreeView object.

Prerequisite

The domain, name, and password of the account to be associated with the Windows-RT service is stored in AppManager Security Manager. AppManager uses these credentials to unlock or login to a computer left in a locked state. AppManager Security Manager stores the information on a per-agent basis. AppManager raises an event if no Security Manager entry is found for an agent.

Complete the following fields in the Custom tab of Security Manager for the Windows agent computer.

Field	Description
Label	`Win-RT7`
Sub-label	`ServiceAccount`
Value 1	Service account domain name
Value 2	Service account name
Value 3	Service account password
Extended application support	Required field. Encrypts the information in Security Manager.

Resource Object

NT_MachineFolder

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed

Description	How To Set It
General	
List of applications to discover, separated by commas	Provide the name of the application you want to discover. To discover more than one application, separate the application names with commas.
Raise event if discovery succeeds?	Select this check box to raise an event when the application or applications listed above are successfully discovered. The default is selected.
Event severity when discovery succeeds	Specify a severity level, from 1 to 40, to indicate the importance of an event if discovery is successful. Default is 25.

Description	How To Set It
Raise event if discovery fails?	Select this check box to raise an event when the application or applications listed above are not successfully discovered. The default is selected.
Event severity when discovery fails	Specify a severity level, from 1 to 40, to indicate the importance of an event if discovery is *not* successful. Default is 5.

WLBS

Use this Knowledge Script to discover the Microsoft Windows Load-Balancing Service clusters and cluster hosts. In general, it is recommended that you install the WLBS managed object and discover (with this Knowledge Script) all of the hosts in the WLBS cluster. Although most Knowledge Scripts can monitor all of the hosts in the cluster if any one host is discovered, some Knowledge Scripts such as RunCommand require you to discover all of the hosts to be able to run a selected command on all hosts within the cluster.

You may need to restart the Operator Console after you discover a WLBS cluster to refresh the cache and ensure the WLBS resource objects are registered before starting WLBS jobs.

Resource Objects

Any WLBS host in the cluster.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have WLBS installed. The default is 15 (yellow event indicator).

WMI

Use this Knowledge Script to discover the Microsoft Windows Management Instrumentation (WMI) server configuration and resources.

Resource Objects

WMI server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have WMI installed. The default is 15 (yellow event indicator).

WRC

Use this Knowledge Script to discover WebTrends Reporting Center installed on Windows servers. This Knowledge Script returns information about successful, failed and partial discoveries and raises events (with user-specified severity) to notify you of errors.

This Knowledge Script may be used to determine if and where WRC instances are installed in a network. It is useful to run this Knowledge Script periodically to detect new instances of WRC and to determine if existing servers have been uninstalled or taken offline.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	Set to **y** to raise an event when the Knowledge Script discovers a WebTrends Server. The default is n.
Event severity when Discovery succeeds	Specify a severity level for the event raised by successful discovery of a WebTrends Server. The default is 35.
Event severity when Discovery fails	Specify a severity level for the event raised by failure to discover a WebTrends Server. The default is 5.

WS.NET

Use this Knowledge Script to automatically discover Web services for .NET resources and configuration information in the local IIS server.

If you installed the Web Services proxy software, Web services running on remote computers can also be discovered.

UDDI Discovery

If you are performing discovery for local services only, use the default settings for the **UDDI Discovery** parameters.

If you are performing discovery for UDDI v2 services, supply the **Inquiry URL** and leave the default settings for the other **UDDI Discovery** parameters.

If you are performing discovery for UDDI v3 services, you must supply the **Inquiry URL**, **Publish URL**, and the **Auth Token** username and password.

Resource Objects

Web services for .NET servers

Default Schedule

By default, this script is only run **once** for each server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	Use the following parameters to determine when events are raised.
Raise event if discovery succeeds?	Set to **Yes** to raise an event if discovery succeeds. By default, events are enabled.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue event indicator).
Raise event if discovery fails?	Set to **Yes** to raise an event if discovery fails. By default, events are enabled.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
UDDI Discovery	Use the following parameters to specify UDDI v2.0 and v3.0 details and enable discovery of UDDI services.
Version	Set the UDDI version, 2.0 or 3.0, for discovering the Web services. The default is 3.0.
Service filter	Enter a service name, or enter a part of the service name preceding or succeeding a wildcard character, to limit the discovery of Web services. The default filter is *.

Parameter	How to Set It
Inquiry URL	Enter the uniform resource locator (URL) of the remote computer where UDDI Registry is been deployed. The default, to illustrate the correct syntax, is as follows: `http://server/registry/uddi/inquiry`
Publish URL	Enter the uniform resource locator (URL) of the server where the service is to be published. The default, to illustrate the correct syntax, is as follows: `http://server/registry/uddi/publish`
Auth Token	Use the following parameters to specify the authentication details of UDDI version 3.0 and above.
Username	Enter the username of the specific UDDI registry.
Password	Enter the password for the specific UDDI registry.

WTS

Use this Knowledge Script to discover Microsoft Windows Terminal Server configuration and resources. If you have Citrix MetaFrame installed on a Windows Terminal Server, you may want to run the MFXP Knowledge Script to discover MetaFrame resources as well.

Resource Objects

Windows Terminal server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have WTS installed. The default is 15 (yellow event indicator).

XenApp

Use this Knowledge Script to discover Citrix XenApp resources and configuration information. The TreeView for this module now includes a reorganized set of objects that include Citrix XenApp or Presentation Server, License Servers, Licenses, Farms, and Servers, along with several additional services: MFCom, Citrix Licensing, Citrix XTE Server, Citrix Service Manager, Citrix Encryption Service, and Citrix IMA Service.

AppManager for Citrix XenApp supports cluster discovery on all cluster nodes for the Citrix License Server component. If you run the Discovery Knowledge Script on both nodes of a cluster added to the Operator Console, the Discovery script discovers the license server on both nodes, but the license types available on the license server object are not discovered. The TreeView for cluster discovery displays the license types available on the License Server object for non-cluster servers only.

Resource Objects

Windows machine objects

Default Schedule

By default, this script is only run **once** for each server.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the discovery job fails. The default is 5.
Event Notification	
Raise event when discovery succeeds?	Select **Yes** to raise an event if the discovery process is successful. The default is unselected.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the discovery process is successful. The default is 21.
Event severity level when discovery partially succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a discovery returns some data but also generates warning messages. The default is 11.

Antigen

Use this Knowledge Script to discover Antigen resource and configuration information.

Resource Objects

Sybari Antigen servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator).

AppCenter

Use this Knowledge Script to discover Microsoft Application Center 2000 configuration and resources.

Resource Objects

Application Center servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have Application Center installed. The default is 15 (yellow event indicator).

BizTalk

Use this Knowledge Script to discover Microsoft BizTalk Server 2000 configuration and resources.

To discover all BizTalk resources, the Logon As account for the NetIQ Client Resource Monitor (`NetIQmc`) must be listed under the BizTalk Server Administrators' Users Group. If the Logon As account does not have this permission, the BizTalk discovery will succeed, but some information will be missing from the Details tab in the Knowledge Script pane of the Operator Console.

Resource Objects

BizTalk servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have BizTalk Server installed. The default is 15 (yellow event indicator).

Commerce

Use this Knowledge Script to discover Microsoft Commerce Server 2000 configuration and resources.

Resource Objects

Commerce servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have Commerce Server installed. The default is 15 (yellow event indicator).

Conference

Use this Knowledge Script to discover Microsoft Exchange 2000 Conferencing Server servers and the services associated with them.

Resource Objects

Exchange 2000 Conferencing Server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity level when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...partially succeeds**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have Veritas Conference installed or does not have the AppManager managed object for Microsoft Exchange 2000 Conferencing Server. The default is 15 (yellow event indicator).

FW1

Use this Knowledge Script to discover Check Point FireWall-1 Management Station and FireWall Module resources. When running the discovery from a Management Station, local and remote Management Stations and FireWall Modules are discovered. When running the discovery from a FireWall Module, only the FireWall Module on the local machine is discovered.

When discovering from a FireWall Module, this Knowledge Script requires a user account and read permissions for Security Rules to enable access to the Management Station database.

Resource Objects

FireWall-1 management stations and FireWall modules.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
FireWall Module Only. LDAP port number.	Enter the LDAP port number used by Check Point FireWall-1 if you are running the discovery on a FireWall Module. The default port number is 18185.
FireWall-1 administrator user ID	When running discoveries from the FireWall Module, enter your FireWall-1 Administrator user ID. The user you enter must have read permissions for Security Rules.
FireWall-1 administrator user password	Enter your FireWall-1 Administrator user password for the user ID entered above.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 21 (blue event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have FireWall-1 installed. The default is 15 (yellow event indicator).

NetShield

Use this Knowledge Script to discover Network Associates NetShield resource and configuration information.

Resource Objects

NetShield servers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have Network Associates NetShield installed. The default is 15 (yellow event indicator).

NetwareManager

Use this Knowledge Script to discover the AppManager for NetWare Mid-Level Manager on an AppManager agent computer. When you drop this Knowledge Script on a managed client, that computer becomes a proxy for monitoring NetWare servers.

You must have NetWare Management Agents and WMI installed in your environment to monitor NetWare servers. You must also edit the configuration file `nwmlm.cfg` to define the information to be collected, the NetWare servers to monitor, and the frequency with which this data is to be collected.

Resource Objects

AppManager for NetWare Mid-Level Managers.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator) • **...is not applicable**. This type of failure usually occurs when the target computer does not have the Mid-Level Manager or NetWare managed object installed. The default is 15 (yellow event indicator).

Site

Use this Knowledge Script to discover Microsoft Site Server configuration and resources.

Resource Objects

Site server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have Site Server installed. The default is 15 (yellow event indicator).

SMS

Use this Knowledge Script to discover Microsoft System Management Server (SMS) configuration and resources. You can run this Knowledge Script on any SMS server. It will determine the version of SMS installed on the target computer. On computers where SMS 2.0 is installed, this Knowledge Script can discover both SMS primary sites and SMS secondary sites.

Resource Objects

SMS server.

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have SMS installed. The default is 15 (yellow event indicator).

Chapter 33
Domino Knowledge Scripts

The Domino category provides Knowledge Scripts for monitoring Lotus Domino servers and Notes mail, including partitioned configurations.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
Connectivity	Monitors mail connectivity between Domino servers.
ConsoleCommand	Issues any Domino server console command.
CPUUtil	Monitors the percentage of CPU resources used by Domino processes.
DbACLChanged	Monitors changes to a database access control list (ACL).
DBCacheHit	Monitors the percentage of data that is read from the Domino database cache.
DBDocNumber	Tracks the number of documents in a Domino database.
DBReplicating	Monitors the rate of successful replications of a Domino database.
DBSizes	Monitors the size of Domino databases, individually or collectively.
DBWhiteSpace	Monitors the whitespace occupied by Domino databases.
GetStat	Monitors any Domino numerical statistics.
HTTPAccessStat	Monitors the number of HTTP access requests for a Domino server and the size of data transferred from the Domino server to a Web client.
InetPortCheck	Monitors the Internet protocol ports used by the Domino server (Internet task).
LogSniff	Checks the Domino log for specific messages or matching search strings.
MailThruput	Monitors the throughput rate of mail messages that are routed through the Domino server.
MemBusy	Monitors the total memory resources used by all Domino processes.
NetworkBusy	Monitors the data sent and received on every Domino network port.
NotesMailStats	Monitors Notes Mail Server (Mail) statistics on Domino servers.

Knowledge Script	What It Does
OldestDocInDB	Monitors the age of documents in a Domino database message queue.
OpenDBResponseTime	Monitors the amount of time required to open a Domino database.
ReplicationTime	Monitors the status of the most recent database replication between Domino servers.
Report_Connectivity	Generates a report about the connectivity and response time between Domino servers.
Report_DatabaseSize	Generates a report about the size of Domino databases.
Report_MailThroughputDeadMails	Generates a report about the number of dead mail messages stored on the Domino server.
Report_MailThruputDeliveredMail	Generates a report about the number of mail messages delivered to the local Domino server.
Report_MailThroughputFailureMail	Generates a report about the number of mail messages that the Domino server failed to deliver.
Report_MailThroughputPendingMails	Generates a report about the number of mail messages sent to the Domino that have yet to be forwarded to their destinations.
Report_MailThroughputRoutedMail	Generates a report about the number of mail messages sent to remote servers and delivered to the local server.
Report_ServerDown	Generates a report about the availability of the Domino server.
Report_ServerUpTime	Generates a report about the up and down time of Domino servers.
Report_TopNDatabases	Generates a report about the Domino databases that use the most disk space on the Domino server.
Report_UserSessions	Generates a report about the number of concurrent user sessions on the Domino server.
ServerAvailability	Monitors changes in the up/down status of a Domino server.
ServerDown	Checks whether a Domino server is down.
SMTPConnectivity	Monitors SMTP mail connectivity between a Domino server and one or more Internet domains.
TaskAvailability	Monitors the status of Domino, third-party, or user add-in tasks.
TaskDown	Monitors the status of Domino, third-party, and user add-in tasks.
TopNAccessDbs	Monitors the top “n” Domino databases that are most frequently accessed on a Domino server.
TopNDatabases	Monitors the Domino databases that use the most disk space on the Domino server.
TopNMailDatabases	Monitors the disk space used by the top user mail files and mail-in databases on the Domino server.
TopNUnUsedDBs	Monitors the size of databases that are not being used.
TopNUsers	Monitors the top “n” users that accessed the Domino server for the longest amount of time.
UserSessions	Monitors the current number of user sessions open on the Domino server.

Connectivity

Use this Knowledge Script to determine whether e-mail can be delivered between Domino servers. This script also tracks the time it takes to receive a response to the test message. This script raises an event if connectivity is down, or if response time exceeds the threshold you specify.

Run this script on the top-level Domino folder in the Operator Console TreeView to test each server's connection to the other servers and to itself, verifying complete connectivity between all Domino servers. When you run this script on one server, the script checks whether the server can send an e-mail to itself and all servers specified on the server list parameter.

Example of Using this Script

To test connectivity, this Knowledge Script sends a test mail message to each server being tested using a local mail database set up for the computer running the job. If the test message is not delivered, the Knowledge Script raises an event to indicate that the server cannot send mail. If the test message delivered by the "sending" server does not get a reply from each "receiving" server within the reply interval you set, the Knowledge Script raises an event indicating connectivity is down.

Run this script on the top-level Domino folder to test each Domino server's connection to the other servers and to itself, verifying complete connectivity between all Domino servers. If you run this script on one server without specifying a destination list, the script simply checks whether the server can send an e-mail to itself in a loop-back fashion.

Note
To use this script, ensure that the Domino server creates the `netiq.nsf` database in the Domino databases. If you do not find `netiq.nsf` under Domino databases, load `nnetiq.exe` on the Domino server. This script uses a special mail-in database for receiving the test messages that verify connectivity.

Performing Periodic Maintenance

You should periodically log in to each Domino server's special NetIQ mail database and mailbox to perform housekeeping, such as removing old mail files. Depending on how frequently you run this script, consider performing these activities weekly or monthly.

Resource Objects

Domino server icon, Domino Server folder

Default Schedule

The default interval is **once every hour**.

If your Domino servers rely on a remote WAN or LAN service (such as RAS) or a dial-up modem that is not always connected, consider setting up server group folders to separate Domino servers into different groups. Then set the schedule interval for this script to run on each folder based on each group's connection schedule.

For example, consider creating one server group for your always-connected servers and a separate folder for offhours RAS connections and create two different sets of jobs with different schedules, frequently for your connected network and once a day or based on the scheduled connection time for the remote access servers.

For more information about setting up server groups, see the *User Guide for AppManager*.

Note
You cannot choose the Run once schedule for this script, which requires at least two job iterations to return useful data.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
List of Domino servers to test connectivity from this server	Provide a list of destination Domino servers for connectivity testing separated by commas. Specify at least one server. For example: `DEV01@LAB01,SALES@LAB02`
Threshold - Maximum response time	Specify the maximum number of seconds from the time the test message is sent out until a reply should be received. If a reply to the test message is not received within this interval, an event is raised. The default is 120 seconds.
Data Collection	
Collect data for connectivity (%) and response time (seconds)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns 100 if the connection is successful and 0 if the connection failed. The default is unselected.
Event Notification	
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of response time exceeds the threshold you set. The default is Yes.
Event severity level when response time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of response time exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Consider using the ServerDown Knowledge Script to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable. The default is 5.

Description	How To Set It
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

ConsoleCommand

Use this Knowledge Script to issue any Domino server console command. This script raises an event if the command returns an output and displays the output of the command in the event details.

Resource Object

Domino server

Default Schedule

The default interval is **every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Domino console command to execute	Specify the console command you want to execute. The default is `Show task`.
Data Collection	
Collect data for command success (%)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of successful commands. The default is unselected.
Event Notification	
Raise event to return command results?	Select **Yes** to raise an event to return command results. The default is Yes.
Event severity level for command results	Set the event severity level, from 1 to 40, to indicate the importance of an event in which command results are returned. The default is 25.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. You should use the ServerDown Knowledge Script to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is unavailable for other reasons such as a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is unavailable for other reasons.The default is 5.

Description	How To Set It
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

CPUUtil

Use this Knowledge Script to monitor the percentage of CPU resources used by Domino processes, including the Domino server and all additional task processes. This script raises an event if CPU usage exceeds the threshold you set.

Resource Object

Domino server

Default Schedule

The default interval is **every 10 minutes**.

Note
You cannot choose the Run once schedule for this script, which requires at least two job iterations to return useful data.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Threshold - Maximum Domino CPU usage	Specify the maximum percentage of CPU that all Domino processes can use before an event is raised. The default is 70%.
Data Collection	
Collect data for Domino CPU usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns CPU usage as a percentage for the monitoring period. The default is unselected.
Event Notification	
Raise event if Domino CPU usage exceeds threshold?	Select **Yes** to raise an event if CPU usage for all Domino processes exceeds the threshold you set. The default is Yes.
Event severity level when Domino CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage for all Domino processes exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use the ServerDown Knowledge Script to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is unavailable for other reasons, such as a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.

Description	How To Set It
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is unavailable for other reasons. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

DbACLChanged

Use this Knowledge Script to monitor changes to a database access control list (ACL). This script raises an event if the ACL changed during the last number of minutes you specify.

Resource Object

Domino server

Default Schedule

The default interval is **once every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
List of databases to monitor	Specify the names of the databases you want to monitor, separating multiple names with commas. The default is the `names.nsf` database.
Number of previous minutes to check	Specify the number of previous minutes to check for changes to the ACL. The default is 60 minutes.
Monitor since last interval? (ignore 'Number of previous minutes to check')	Select **Yes** to check for the changes to the ACL that have been added since the last interval. If set to Yes, the value specified in the *Number of previous minutes to check* parameter is ignored. The default is unselected.
Data Collection	
Collect data for number of changed ACLs?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number changes that occurred in the ACL during the period you specified. The default is unselected.
Event Notification	
Raise event if database ACLs changed?	Select **Yes** to raise an event if a database ACL has been changed. The default is unselected.
Event severity level if database ACLs changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which changes to the ACL have occurred. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. You should use the ServerDown Knowledge Script to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is unavailable for other reasons, such as a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.

Description	How To Set It
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is unavailable for other reasons. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

DBCacheHit

Use this Knowledge Script to monitor the percentage of data read from the Domino database cache. Because retrieving data from the database cache is typically faster and more efficient than accessing database tables directly, this script provides a good indicator of database performance.

Resource Object

Database folder (top-level)

Default Schedule

The default interval is **every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Threshold - Minimum database cache hit rate	Specify the minimum percentage of data that should be read from the Domino database cache. Ideally, this percentage should be set relatively high, because the more frequently Domino uses the data cache, the better your database performance. This script raises an event when the percentage of cache data accessed falls below the threshold you set. The default is 50%.
Data Collection	
Collect data for database cache hit rate (%)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the rate at which the database cache was accessed during the monitoring period. The default is unselected.
Event Notification	
Raise event if database cache hit rate falls below threshold?	Select **Yes** to raise an event if the database cache access rate falls below the threshold you set. The default is Yes.
Event severity level when database cache hit rate falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the database cache access rate falls below the threshold you set. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. You should use the ServerDown Knowledge Script to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is unavailable for other reasons, such as a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.

Description	How To Set It
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is unavailable for other reasons. The default is 5.
Collect data as ‘-1’ for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a “hung” Domino Server or nnetiq task will not “hang” this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

DBDocNumber

Use this Knowledge Script to monitor the number of documents in a Domino database. This script raises an event if the number of documents exceeds the threshold you set.

Resource Object

Domino server

Default Schedule

The default interval is **once every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Name of database to monitor	Specify the name of the database you want to monitor. The default is `log.nsf`.
View name or formula for monitored database	Specify the database view name or selection formula to use. The default is `SELECT FORM = ""Events""` to filter on event documents. To use a view name instead, type `VIEW = ""name""`.
Threshold - Maximum number of documents	Specify the maximum number of documents that can be in the database before an event is raised. The default is 1000 documents.
Data Collection	
Collect data for number of documents in database?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of documents in the database during the monitoring period. The default is unselected.
Event Notification	
Raise event if number of documents exceeds threshold?	Select **Yes** to raise an event if the number of documents in the database exceeds the threshold you set. The default is Yes.
Event severity level when number of documents exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of documents in the database exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. You should use the ServerDown Knowledge Script to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is unavailable for other reasons, such as a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.

Description	How To Set It
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is unavailable for other reasons. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

DBReplicating

Use this Knowledge Script to monitor the rate of successful replications of a Domino database. This script raises an event if the percentage of successful replications falls below the threshold you set, or if statistics are not available.

Resource Object

Domino server

Default Schedule

The default interval is **once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Threshold - Minimum successful replication	Specify the minimum percentage of database replications that should be successful to prevent an event from being raised. The default is 75%.
Data Collection	
Collect data for successful replication (%)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of successful replications for the monitoring period. The default is unselected.
Event Notification	
Raise event if successful replication rate falls below threshold?	Select **Yes** to raise an event if the percentage of successful database replications falls below the threshold you set. The default is Yes.
Event severity level if successful replication rate falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of successful replications falls below the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable for other reasons. The default is 5.

Description	How To Set It
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

DBSizes

Use this Knowledge Script to monitor the size of Domino databases. Run this script on an individual database to monitor the size of that database. Run this script on a database folder to monitor the size of each database in the folder and the total size of all databases together. This script raises an event if the individual database size or total database size exceeds the threshold you set.

Resource Objects

Database icons, Database folder

Default Schedule

The default interval is **once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Threshold - Maximum total databases size	Specify the maximum file size that all databases can attain before an event is raised. The default is 1000 MB.
Threshold - Maximum individual database size	Specify the maximum file size that individual databases can attain before an event is raised. The default is 50 MB.
Use file specification for the list of databases to monitor?	Select **Yes** to specify the list of databases you are monitoring.
Full path to files for each server with list of databases	Provide the full path to the file name that contains the database names you are monitoring. For example: `<HKLM\SOFTWARE\NetIQ\AppManager\4.0\InstallPath>\Discovery_<SERVER>.txt` **Note** Each database name must be mentioned in a separate line in the text file.
Data Collection	
Collect data for total size of all databases (MB)?	Select **Yes** to collect the total file size for all databases you are monitoring. The default is unselected.
Collect data for size of each database (MB)?	Select **Yes** to collect the file size for each monitored database. The default is unselected.
Event Notification	
Raise event if total size of all databases exceeds threshold?	Select **Yes** to raise an event if the total size of all databases exceeds the threshold you set. The default is Yes.
Event severity level when total size of all databases exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the size of all databases exceeds the threshold. The default is 5.
Raise event if size of individual databases exceeds threshold?	Select **Yes** to raise an event if the size of an individual database exceeds the threshold you set. The default is Yes.

Description	How To Set It
Event severity level when size of individual databases exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the size of an individual databases exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is unavailable for other reasons. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

DBWhiteSpace

Use this Knowledge Script to monitor the whitespace occupied by Domino databases. Database whitespace is disk space that the operating system allots to Domino but which Domino does not use. This script raises an event if the amount of whitespace and percentage of whitespace exceed the thresholds you set. You can choose to automatically initiate database compaction.

Resource Objects

Database icons, Database folder

Default Schedule

The default interval is **once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Threshold - Maximum whitespace size	Specify the maximum amount of whitespace that a Domino database can occupy before an event is raised. The default is 50 MB.
Threshold - Maximum whitespace percentage	Specify the maximum percentage of whitespace that can be allocated to a Domino database before an event is raised. The default is 10%.
Use file specification for the list of databases to monitor?	Select **Yes** to specify a full path to the list of databases you want to monitor.
Full path to files for each server with list of databases	Provide the full path to the file that contains the database names you want to monitor. For example: `<HKLM\SOFTWARE\NetIQ\AppManager\4.0\InstallPath>\Discovery_<SERVER>.txt` **Note** Mention each database name in a separate line in the text file.
Data Collection	
Collect data for whitespace size and percentage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the size (in MB) and percentage of whitespace. The default is unselected.
Event Notification	
Raise event if whitespace exceeds both size and percent thresholds?	Select **Yes** to raise an event if whitespace size and whitespace percentage exceed the thresholds you set. The default is Yes.
Event severity level when whitespace exceeds both size and percent thresholds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which whitespace size and percentage exceeds the thresholds. The default is 5.
Raise event if error occurs during database compaction?	Select **Yes** to raise an event if an error occurs during database compaction. The default is Yes.
Event severity level when error occurs during database compaction	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an error occurs during database compaction. The default is 5.
Operations	

Description	How To Set It
Compact database if whitespace exceeds both size and percent thresholds?	Select **Yes** to automatically compact the database to free up disk space when whitespace exceeds both the size and percentage thresholds. The default is unselected.
Maximum wait time for all database compactions	Specify the maximum number of minutes this script waits for applicable database compactions to occur. If sufficient time is not allowed, only some of the database compactions may occur. For this reason, you can choose not to automatically compact databases. Instead, when events indicate you should implement compaction, run this script on individual databases.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable for other reasons. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

GetStat

Use this Knowledge Script to monitor Domino numerical statistics. You can specify a threshold value for any statistics you are monitoring. You cannot use this script to monitor statistics that return string or list data.

Resource Object

Domino server

Default Schedule

The default interval is **once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Domino statistic name to monitor	Provide the name of a Domino statistic that returns numerical data. For example `Server.Sessions.Dropped`. To get a list of statistics names, from a Domino client open the `events4.nsf` database and look under Names and Messages. Click **Statistic Names**. The default statistic is `Server.Tasks`.
Threshold - Maximum statistic value	Specify the maximum value that can be returned by a monitored statistic before an event is raised. The default is 1000.
Data Collection	
Collect data for numerical statistic value?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the value of the monitored statistic. The default is unselected.
Event Notification	
Raise event if statistic value exceeds threshold?	Select **Yes** to raise an event if a statistic value exceeds the threshold you set. The default is Yes.
Event severity level when statistic value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the value of a monitored statistic exceeds the threshold. The default is 5.
Raise event if statistic not found?	Select **Yes** to raise an event if the statistic does not exist on the monitored server. The default is Yes.
Event severity level when statistic not found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a statistic does not exist on the monitored server. The default is 25.
Cancel job if statistic not found?	Select **Yes** to cancel the Knowledge Script job if the statistic does not exist on the monitored server. The default is Yes.
Event severity level when statistic not found and job canceled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the statistic cannot be found and the Knowledge Script job is canceled. The default is 5.
Data Acquisition Problems	

Description	How To Set It
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from the nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event if the data is unavailable for other reasons. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

HTTPAccessStat

Use this Knowledge Script to monitor the number of HTTP access requests for a Domino server and the size of data transferred from the Domino server to a Web client. This script raises an event when either the number of HTTP requests or maximum file size exceeds the threshold values you specify.

To use this script, enable the Domino Web server log (`domlog.nsf`) database in the Domino server. For more information about enabling logs in the Domino server, see the Lotus Domino server documentation.

If the Domino server cannot locate `domlog.nsf`, it tries to locate any of the following log files:

```
access<mmddyyyy>.log
agent<mmddyyyy>.log
referrer<mmddyyyy>.log
```

where `mm` is the month the Domino server creates the log file, `dd` is the date the Domino server creates the log file, and `yyyy` is the year the Domino server creates the log file.

This script raises an event if log files cannot be located.

Tip
Domino often delays purging log file data until midnight, so run this script just after midnight.

Resource Object

Domino server

Default Schedule

The default interval is **once every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Number of previous hours to monitor	Specify the number of previous hours to monitor access requests. The default is 24 hours.
Threshold - Maximum number of HTTP requests	Specify the maximum number of HTTP requests that should be answered by the Domino server before an event is raised. The default is 10000 requests.
Threshold - Maximum amount of transferred data	Specify the maximum file size that transferred files can attain before an event is raised. The default is 1000 MB.
Data Collection	
Collect data for number of HTTP requests?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of HTTP requests during the monitoring period. The default is unselected.
Collect data for amount of transferred data (MB)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the size of transferred files during the monitoring period. The default is unselected.

Description	How To Set It
Event Notification	
Raise event if number of HTTP requests exceeds threshold?	Select **Yes** to raise an event if the number of HTTP requests exceeds the threshold you set. The default is Yes.
Event severity level when number of HTTP requests exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of HTTP requests exceeds the threshold. The default is 5.
Raise event if amount of transferred data exceeds threshold?	Select **Yes** to raise an event if the amount of transferred data exceeds the threshold you set. The default is Yes.
Event severity level when amount of transferred data exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of transferred data exceeds the threshold. The default is 25.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable for other reasons. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

InetPortCheck

Use this Knowledge Script to monitor the Internet protocol ports used by the Domino server (Internet task). You can specify which protocol ports to check. This script raises an event if a monitored port is enabled but inactive.

Resource Object

Domino server

Default Schedule

The default interval is **every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Event Notification	
Raise event if the HTTP port is enabled but inactive?	Select **Yes** to check the HTTP server port. The default is Yes.
Raise event if the LDAP port is enabled but inactive?	Select **Yes** to check the LDAP server port. The default is Yes.
Raise event if the NNTP port is enabled but inactive?	Select **Yes** to check the NNTP server port. The default is Yes.
Raise event if the IMAP port is enabled but inactive?	Select **Yes** to check the IMAP server port. The default is Yes.
Raise event if the POP3 port is enabled but inactive?	Select **Yes** to check the POP3 server port. The default is Yes.
Event severity level when ports are enabled but inactive	Set the event severity level, from 1 to 40, to indicate the importance of an event in which ports are inactive. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable for other reasons. The default is 5.

Description	How To Set It
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

LogSniff

Use this Knowledge Script to monitor the Notes log database for specific messages or search strings. You enter the search strings to look for using two filter files: the **Include Description File** and the **Exclude Description File**. These files contain the search strings you want to include or exclude, respectively. The search strings can include regular expressions.

You can use just the Include filter file, just the Exclude filter file, or both. If you use both filter files, this script returns messages that contain any included search strings and do not contain any of the excluded search strings. This script raises an event if the number of matching messages found exceeds the threshold you set. This script returns the items that match the search criteria that are new since the last time the script ran.

Note
The Description Files must be available locally on the computer where this script runs.

Resource Object

Domino server

Default Schedule

The default interval is **once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Form name to monitor in log database	Provide the form name of the `Notes` log database you want to search. The script searches for messages in the log document of this type. The default form name is Events.
Full path to file containing include strings	Provide the full path to the file name that contains the search strings you want to include. For example: `C:\logsearch\include.txt`
Full path to file containing exclude strings	Provide the full path to the name of the file that contains the search strings you want to exclude. For example: `C:\logsearch\exclude.txt`
Search type to apply	Specify the search type that you want to apply to the strings in the file: • **Automatic** - Select this search type to let the system automatically include strings to compare from a file. • **Literals** - Select this search type when the string in the search file is the literal value that has to be compared. • **RegularExpression** - Select this search type when the string in the search file is a regular expression. By default, the default search type is Automatic.
Previous 24-hour periods to search (for Run Once)	Normally, this script scans for log messages that are new since the last interval. If you schedule the script to Run Once, enter the number of previous days to scan the log for messages. The default is 1 Day.

Description	How To Set It
Threshold - Maximum number of matching messages	Specify the maximum number of matching messages to collect before raising an event. The default is 100 matching items.
Data Collection	
Collect data for number of matching messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of matching messages in the log. The default is unselected.
Event Notification	
Raise event if number of matching messages exceeds threshold?	Select **Yes** to raise an event if the number of matching messages exceeds the threshold you set. The default is Yes.
Event severity level when number of matching messages exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of matching messages exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable for other reasons. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

MailThruput

Use this Knowledge Script to monitor the throughput rate of mail messages that are routed through the Domino server. This script monitors the number of routed, dead, and pending mail messages. This script raises an event if threshold values are exceeded.

Routed mail includes all of the mail messages sent to remote servers and all mail messages delivered to the local server. **Pending mail** messages are messages sent to the Domino server that have not yet been sent by the server to their destination.

When the Domino server cannot complete the delivery of mail and is not able to notify the sender of the mail delivery problem with an error message, the mail is stored on the server and flagged as **dead mail**.

Example of How This Script is Used

This script provides insight into the overall health of your mail delivery system by monitoring dead and pending mail as well as the number of successfully routed messages. In addition, you can use these thresholds and associated events to help you determine when to perform housekeeping tasks such as deleting old mail messages.

Resource Objects

Domino mail routers for Notes

Default Schedule

The default interval is **every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Threshold - Maximum routed messages this interval	Specify the maximum number of mail messages that can be routed through the Domino server before an event is raised. Threshold applies to the sum of mail delivered to the server and mail transferred from the server to other destinations. The default is 1000 mail messages.
Threshold - Maximum total dead messages	Specify the maximum number of dead mail messages that can occur before an event is raised. The default is 10 messages.
Threshold - Maximum total waiting messages	Specify the maximum number of pending mail messages that can occur before an event is raised. The default is 100 messages.
Data Collection	
Collect data for dead messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of dead mail messages. The default is unselected.
Collect data for pending messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of pending mail messages. The default is unselected.
Collect data for delivered messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of delivered mail messages. The default is unselected.

Description	How To Set It
Collect data for routed messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of routed mail messages. The default is unselected.
Collect data for failed messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of failed mail messages. The default is unselected.
Event Notification	
Raise event if routed messages exceed threshold?	Select **Yes** to raise an event if the number of routed messages exceeds the threshold you set. The default is Yes.
Event severity level when routed messages exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of routed messages exceeds the threshold. The default is 5.
Raise event if dead messages exceed threshold?	Select **Yes** to raise an event if the number of dead messages exceeds the threshold you set. The default is Yes.
Event severity level when dead messages exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event if the number of dead messages exceeds the threshold. The default is 5.
Raise event if waiting messages exceed threshold?	Select **Yes** to raise an event if the number of waiting messages exceeds the threshold you set. The default is Yes.
Event severity level when waiting messages exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of waiting messages exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable for other reasons. The default is 5.

Description	How To Set It
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

MemBusy

Use this Knowledge Script to monitor the total memory resources used by all Domino processes. This script raises an event if the amount of memory used exceeds the threshold you set.

Resource Object

Domino server

Default Schedule

The default interval is **every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Threshold - Maximum Domino memory usage	Specify the maximum amount of memory that can be used by all Domino processes before an event is raised. The default is 20000 KB.
Data Collection	
Collect data for Domino memory usage (KB)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of memory usage for all Domino processes. The default is unselected.
Event Notification	
Raise event if memory usage exceeds threshold?	Select **Yes** to raise an event if memory usage exceeds the threshold you set. The default is Yes.
Event severity level when memory usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable for other reasons. The default is 5.

Description	How To Set It
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

NetworkBusy

Use this Knowledge Script to monitor the data sent and received on every Domino network port. This script raises an event if the amount of data sent and received on any Domino network port exceeds the thresholds you set.

Resource Object

Domino server

Default Schedule

The default interval is **every 30 minutes**.

Note
You cannot choose the Run once schedule for this script, which requires at least two job iterations to return useful data.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Threshold - Maximum amount of data sent from any port	Specify the maximum amount of data that can be sent on a Domino network port before an event is raised. The default is 10000 KB.
Threshold - Maximum amount of data received from any port	Specify the maximum amount of data that can be received on a Domino network port before an event is raised. The default is 10000 KB.
Data Collection	
Collect data for total amount of data sent and received per port?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total amount of data sent and received per port during the monitoring period. The default is unselected.
Event Notification	
Raise event if amount of data sent or received exceeds threshold?	Select **Yes** to raise an event if amount of the amount of data sent or received exceeds the threshold you set. The default is Yes.
Event severity level when amount of data sent or received exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of data sent or received exceeds the threshold. The default is 5.
Raise event if data not found?	Select **Yes** to raise an event if no data is found. The default is Yes.
Event severity level when data not found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no data is found. The default is 25.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.

Description	How To Set It
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable for other reasons. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

NotesMailStats

Use this Knowledge Script to monitor Notes Mail Server statistics on Domino servers:

- Mail.Dead
- Mail.Waiting
- Mail.TransferFailure
- Mail.Delivered
- Mail.AverageDeliverTime
- Mail.TotalRouted
- Mail.TotalKBTransferred.

This script extracts values from these statistics and raises an event if a threshold is exceeded.

Resource Object

Domino server

Default Schedule

The default interval is **once an hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Threshold - Maximum dead mail messages	Specify the maximum number of dead mail messages (Mail.Dead) that can occur before an event is raised. The default is 1000 messages.
Threshold - Maximum waiting mail messages	Specify the maximum number of mail messages that can be waiting to be routed (Mail.Waiting) before an event is raised. The default is 1000 messages.
Threshold - Maximum failed transfer messages	Specify the maximum number of mail messages that the server can fail to route (Mail.TransferFailures) before an event is raised. The default is 1000 messages.
Threshold - Maximum delivered mail messages	Specify the maximum number of mail messages that can be delivered to mailboxes on the server (Mail.Delivered) before an event is raised. The default is 1000 messages.
Threshold - Maximum average message delivery time	Specify the maximum average time it can take to deliver a mail message (Mail.AverageDeliverTime) before an event is raised. The default is 1000 seconds.
Threshold - Maximum routed mail messages	Specify the maximum number of mail messages that can be routed to or from other servers (Mail.TotalRouted) before an event is raised. The default is 1000 messages.
Threshold - Maximum total KB transferred	Specify the maximum number of bytes that can be transferred by the server for all mail messages (Mail.TotalKBTransferred) before an event is raised. The default is 1000 KB.

Description	How To Set It
Data Collection	
Collect data for number of dead mail messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of dead mail (Mail.Dead) messages. The default is unselected.
Collect data for number of waiting mail messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of waiting mail messages (Mail.Waiting). The default is unselected.
Collect data for number of transfer failures?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of mail messages that failed to be transferred (Mail.TransferFailures). The default is unselected.
Collect data for number of delivered mail messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of delivered mail messages (Mail.Delivered). The default is unselected.
Collect data for average message delivery time?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average delivery time (in seconds) for mail messages (Mail.AverageDeliverTime). The default is unselected.
Collect data for number of routed mail messages?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of routed mail messages (Mail.TotalRouted). The default is unselected.
Collect data for total KB transferred?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total amount (in KB) of transferred mail messages (Mail.TotalKBTransferred). The default is unselected.
Event Notification	
Raise event if dead mail exceeds threshold?	Select **Yes** to raise an event if the number of dead mail messages (Mail.Dead) exceeds the threshold. The default is Yes.
Event severity level when dead mail exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of dead messages exceeds the threshold. The default is 5.
Raise event if waiting mail exceeds threshold?	Select **Yes** to raise an event if the number of waiting messages (Mail.Waiting) exceeds the threshold. The default is Yes.
Event severity level when waiting mail exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of waiting messages exceeds the threshold. The default is 5.
Raise event if message transfer failures exceed threshold?	Select **Yes** to raise an event if the number of message transfer failures (Mail.TransferFailures) exceeds the threshold. The default is Yes.
Event severity level when message transfer failures exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of message transfer failures exceeds the threshold. The default is 5.
Raise event if delivered mail exceeds threshold?	Select **Yes** to raise an event if the number of delivered messages (Mail.Delivered) exceeds the threshold. The default is Yes.
Event severity level when delivered mail exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of delivered messages exceeds the threshold. The default is 5.
Raise event if average mail delivery time exceeds threshold?	Select **Yes** to raise an event if average message delivery time (Mail.AverageDeliverTime) exceeds the threshold. The default is Yes.
Event severity level when average mail delivery time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average message delivery time exceeds the threshold. The default is 5.

Description	How To Set It
Raise event if routed mail exceeds threshold?	Select **Yes** to raise an event if the number of routed messages (Mail.TotalRouted) exceeds the threshold. The default is Yes.
Event severity level when routed mail exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of routed messages exceeds the threshold. The default is 5.
Raise event if total KB transferred exceeds threshold?	Select **Yes** to raise an event if the amount (in KB) of transferred messages (Mail.TotalKBTransferred) exceeds the threshold. The default is Yes.
Event severity level when total KB transferred exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of transferred messages exceeds the threshold. The default is 5.
Event severity level when no data available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no mail statistics are available. The default is 25.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable for other reasons. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

OldestDocInDB

Use this Knowledge Script to monitor the age of documents in a Domino database message queue. You can specify a threshold age for documents in the queue. This script raises an event if a document is older than the threshold age you specified.

Resource Object

Domino server

Default Schedule

The default interval is **once every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Database to monitor	Provide the name of the database to monitor. The default is `netiq.nsf`. You can specify only one database name.
Threshold - Maximum document age	Specify the maximum age that a document can attain before an event is raised. In other words, indicate the longest amount of time a document can remain in the message queue. The default is 1000 seconds.
Data Collection	
Collect data for oldest document age (seconds)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the age of the oldest documents in the queue. The default is unselected.
Event Notification	
Raise event if document age exceeds threshold?	Select **Yes** to raise an event if the document age exceeds the threshold you set. The default is Yes.
Event severity level when document age exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event if the age of a document exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable for other reasons. The default is 5.

Description	How To Set It
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

OpenDBResponseTime

Use this Knowledge Script to monitor the amount of time required to open a Domino database (response time). You can set a threshold value in seconds for the amount of time required for a database to open. This script raises an event if the time to open a monitored database exceeds the response time you set.

Resource Object

Domino server

Default Schedule

The default interval is **once every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Databases to monitor	Specify the names of one or more databases to monitor, separated by commas. The default is `names.nsf:People`.
Threshold - Maximum response time	Specify the maximum amount of time it can take to open a Domino database before an event is raised. The default is 5 seconds.
Data Collection	
Collect data for response time (seconds)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of response time during the monitoring period. The default is unselected.
Event Notification	
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of response time exceeds the threshold you set. The default is Yes.
Event severity level when response time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of response time exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable for other reasons. The default is 5.

Description	How To Set It
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

ReplicationTime

Use this Knowledge Script to monitor the status of database replications between Domino servers, including the time used to complete replication and the name of the changed database. The detail message includes the total time taken for replication to complete. This script raises an event if replication does not complete successfully, and records the cause of the failure in the detail message.

Only replications initiated by the local Domino server are monitored. To monitor replications initiated by other servers, run this script on those servers instead.

Note
Turn on the local Replication Log to use this script.

Resource Object

Domino server

Default Schedule

The default interval is **once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Servers to which the local server initiates replication	Provide a list of Domino servers where replication takes place. Separate the server names by commas. Provide at least one server name. If a server is in a different Domino domain than the server running this script, include the domain name. For example: `DEV01,LAB01,SALES\LAB02`.
Threshold - Maximum replication time	Specify the maximum amount of time that replication can take before an event is raised. The default is 20 minutes.
Number of previous hours to monitor	Specify the number of previous hours to monitor for replications initiated by the local server. The default is 1 hour.
Data Collection	
Collect data for total replication time?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of replication time for the monitoring period. The default is unselected.
Event Notification	
Raise event if replication time exceeds threshold?	Select **Yes** to raise an event if the amount of replication time exceeds the threshold you set. The default is Yes.
Event severity level when replication time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of replication time exceeds the threshold. The default is 5.
Raise event if no replication during period?	Select **Yes** to raise an event if no replication occurs during the monitoring period. The default is unselected.

Description	How To Set It
Event severity level when no replication during period	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no replication occurs during the monitoring period. The default is 25.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data is unavailable for other reasons. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

Report_Connectivity

Use this Knowledge Script to generate a report about the connectivity and response time between Domino servers. This report uses data collected by the Connectivity Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select computers	Select the computers to include in your report.
Select time range	Set a specific or sliding time range for data to include in your report.
Select peak weekdays	Select the days of the week to include in your report.
Data Settings	
Hours or percentage on chart	Select whether to illustrate availability by number of hours or by percentage.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Specify a value for either the percentage or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Report Settings	
Include parameter help table?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include data stream table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include data stream chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.

Description	How To Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties. The default report title is Domino Connectivity.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Raise event if report succeeds?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Severity level when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has no data. The default is 25.
Severity level when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_DatabaseSize

Use this Knowledge Script to generate a report about the size of Domino databases. Use this report to make a statistical analysis of the data point values, such as the average or maximum value over a specified period. This report uses data collected by the DBSizes Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select computers	Select the computers to include in your report.
Select time range	Set a specific or sliding time range for data to include in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data Settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a value for either the percentage or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to yes, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report Settings	
Include parameter help table?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include data stream table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include data stream chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties. The default report title is Domino Mail Database Sizes MB.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Raise event if report succeeds?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Severity level when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has no data. The default is 25.
Severity level when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_MailThroughputDeadMails

Use this Knowledge Script to generate a report about the number of dead mail messages stored on the Domino server. Use this report to make a statistical analysis of the data point values, such as the average or maximum value over a specified period. This report uses data collected by the MailThruput Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select computers	Select the computers to include in your report.
Select time range	Set a specific or sliding time range for data to include in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data Settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a value for either the percentage or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to yes, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report Settings	
Include parameter help table?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include data stream table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include data stream chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties. The default report title is Domino Mail Throughput Dead Mails.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event if report succeeds?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Severity level when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has no data. The default is 25.
Severity level when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_MailThroughputFailureMail

Use this Knowledge Script to generate a report about the number of mail messages that the Domino server failed to deliver. Use this report to make a statistical analysis of the data point values, such as the average or maximum value over a specified period. This report uses data collected by the MailThruput Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select computers	Select the computers to include in your report.
Select time range	Set a specific or sliding time range for data to include in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data Settings	

Description	How To Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Specify a value for either the percentage or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to yes, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help table?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include data stream table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include data stream chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.

Description	How To Set It
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties. The default report title is Domino Mail Throughput Failure Mail.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event if report succeeds?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Severity level when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has no data. The default is 25.
Severity level when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_MailThroughputPendingMails

Use this Knowledge Script to generate a report about the number of mail messages sent to the Domino server that have yet to be forwarded to their destinations. Use this report to make a statistical analysis of the data point values, such as the average or maximum value over a specified period. This report uses data collected by the MailThruput Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select computers	Select the computers to include in your report.
Select time range	Set a specific or sliding time range for data to include in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data Settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a value for either the percentage or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to yes, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report Settings	
Include parameter help table?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include data stream table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include data stream chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties. The default report title is Domino Mail Throughput Pending Mails.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event if report succeeds?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Severity level when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has no data. The default is 25.
Severity level when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_MailThroughputRoutedMail

Use this Knowledge Script to generate a report about the number of mail messages sent to remote servers and delivered to the local server. Use this report to make a statistical analysis of the data point values, such as the average or maximum value over a specified period. This report uses data collected by the MailThruput Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select computers	Select the computers to include in your report.
Select time range	Set a specific or sliding time range for data to include in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data Settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a value for either the percentage or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to yes, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report Settings	
Include parameter help table?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include data stream table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include data stream chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties. The default report title is Domino Mail Throughput Routed Mail.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event if report succeeds?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Severity level when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has no data. The default is 25.
Severity level when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_MailThruputDeliveredMail

Use this Knowledge Script to generate a report about the number of mail messages delivered to the local Domino server. Use this report to make a statistical analysis of the data point values, such as the average or maximum value over a specified period. This report uses data collected by the MailThruput Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select computers	Select the computers to include in your report.
Select time range	Set a specific or sliding time range for data to include in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a value for either the percentage or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to yes, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help table?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include data stream table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include data stream chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties. The default report title is Domino Mail Throughput Delivered Mail.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event if report succeeds?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Severity level when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has no data. The default is 25.
Severity level when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_ServerDown

Use this Knowledge Script to generate a report about the availability of the Domino server. This report uses data collected by the ServerDown Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select computers	Select the computers to include in your report.
Select time range	Set a specific or sliding time range for data to include in your report.
Select peak weekdays	Select the days of the week to include in your report.
Data Settings	
Hours or percentage on chart	Select whether to illustrate availability by number of hours or by percentage.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Specify a value for either the percentage or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Report Settings	
Include parameter help table?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include data stream table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include data stream chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.

Description	How To Set It
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties. The default report title is Domino Server Down.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event if report succeeds?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Severity level when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has no data. The default is 25.
Severity level when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_ServerUpTime

Use this Knowledge Script to generate a report detailing the up and down time of monitored Domino servers. Up and down times are shown in hours and minutes, as well as the percentage of the monitoring interval during which a computer is running or not running. For example, if during a 24-hour monitoring interval, the computer is running for 18 hours and not running for six hours, the up and down times are represented as:

- Up Time: 18 hours 0 minutes
- Down Time: 6 hours 0 minutes
- Up Time: 75%
- Down Time: 25%

This report uses data collected by the ServerAvailability Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select data streams	Select the data streams to include in your report. **Note** It is recommended to choose “By Data Stream” for this parameter.
Select the style	Select the style for the first page of the report: • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data to include in your report.
Select peak weekdays	Select the days of the week to include in your report.
Aggregation interval	Select the period by which the data in your report is aggregated: • Hourly • Daily • Weekly
Report Settings	
Include parameter help table?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include data stream table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include data stream chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.

Description	How To Set It
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Select **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties. The default report title is Domino Server Up Time.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Raise event if report succeeds?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Severity level when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has no data. The default is 25.
Severity level when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_TopNDatabases

Use this Knowledge Script to generate a report about the Domino databases that use the most disk space on the Domino server. This report uses data collected by the TopNDatabases Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select computers	Select the computers to include in your report.
Select time range	Set a specific or sliding time range for data to include in your report.
Report settings	
Include parameter help table?	Set to **Yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Select output folder	Set properties for the output folder.
Select properties	Set miscellaneous report properties. The default report title is Domino Top N Databases Information.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event if report succeeds?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Severity level when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has no data. The default is 25.
Severity level when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_UserSessions

Use this Knowledge Script to generate a report about the number of concurrent user sessions on the Domino server. Use this report to make a statistical analysis of the data point values, such as the average or maximum value over a specified period. This report uses data collected by the UserSessions Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Source	
Select computers	Select the computers to include in your report.
Select time range	Set a specific or sliding time range for data to include in your report.
Select peak weekdays	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data Settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report

Description	How To Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a value for either the percentage or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to yes, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help table?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include data stream table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include data stream chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set properties for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties. The default report title is Domino User Sessions.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event Notification	
Raise event if report succeeds?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.

Description	How To Set It
Severity level when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has no data. The default is 25.
Severity level when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report cannot be generated. The default is 5.

ServerAvailability

Use this Knowledge Script to monitor changes in the up and down status of a Domino server. This script raises an event when the server is up or when the server is down.

This script collects the data used by the Report_ServerUpTime script. The data can be used by other Report scripts, as well.

Resource Object

Domino server

Default Schedule

The default interval is **every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Collection	
Collect data for instance and overall availability (%)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of server availability during the monitoring period. The default is unselected.
Event Notification	
Event severity level when server is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a server is down. The default is 5.
Event severity level when server is up	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a server is up. The default is 15.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level if nnetiq task is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.

Description	How To Set It
Event severity level when data is otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is otherwise unavailable. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.

ServerDown

Use this Knowledge Script to determine whether a Domino server is down. This script raises an event if the server is down.

Resource Object

Domino server

Default Schedule

The default interval is **every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Data Collection	
Collect data for availability (%)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns 100 if the server is up, 50 if the server is restarting, or 0 if the server s down. The default is unselected.
Event Notification	
Raise event if Domino server is down?	Select **Yes** to raise an event if the Domino server is down. The default is Yes.
Event severity level when server is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Domino server is down. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is otherwise unavailable. The default is 5.

Description	How To Set It
Collect data as ‘-1’ for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a “hung” Domino Server or nnetiq task will not “hang” this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

SMTPConnectivity

Use this Knowledge Script to verify connectivity between a Domino server and one or more Internet domains. This script raises an event if connectivity is down.

To configure this script, you need to know the keyword strings that appear in a non-delivery report (NDR) subject and body when the domain is available (up) and, optionally, when the domain is unavailable (down).

A *non-delivery report* is a notice that a message was not delivered to the recipient. This script uses specified search criteria to determine the host status from the non-delivery report. A non-delivery report is created when:

- The test message was successfully sent to the host computer, but the user does not exist on the host computer. In this case, SMTP connectivity is available (up).
- The test message was unsuccessfully sent to the host computer, for example, because the host address is not available. In this case, connectivity to the host is not available (down).

Note
This script sends a test message to the abcdefg123 user at one or more specified domains, for example abcdefg123@netiq.com. In the likely event that the user does not exist on the host computer, an NDR is sent to the NetIQ mailbox.

Before Running this Knowledge Script

Before you begin, determine the SMTP host status from an NDR. The NDR must contain a text string in the subject line of the message that identifies the host status. Typically, the subject text in an NDR varies with each domain. After receiving an NDR, review the subject line of the message. The subject line must contain a keyword string that identifies the host status. For example, `user account inactive` indicates the host computer is available, but the user does not exist on the host computer. A subject such as `no route` indicates connectivity is down.

Understanding How Keyword Strings Work

AppManager compares the text in the subject of the NDR to the specified keyword strings for the host status parameters in the script.

The specified keyword strings must match the actual string that appears in the NDR, including spaces. AppManager searches the subject line from left to right. The search is not case-sensitive.

When specifying one or more host status parameters, note the following:

If a text string in the NDR matches* the keyword string specified for	AppManager reports the status as
Subject keywords when host is up	Up
Subject keywords when host is down	Down
Subject keywords when host is both up and down	Down

Note
By default, this script sends a test message to one or more specified domains using the abcdefg123 user name. This user name may appear in the NDR subject or body.

Performing Routine Maintenance

Periodically remove old messages from the Domino server's mailbox and the NetIQ mail database.

Resource Object

Domino server

Default Schedule

The default interval for this script is **once every hour**.

Note
You cannot choose the Run once schedule for this script, which requires at least two job iterations to return useful data.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Internet domains to monitor	Specify the domain names that you want to check. If specifying more than one, the order in which you specify the Internet domains must correspond to the list of Subject and Body Keywords. Separate more than one entry with an "|"; do not use spaces. For example, `netiq.com|abc.com`. The default is `netiq.com`.
NDR subject phrase identifying host is up	Provide a keyword string that should appear in the NDR subject when the host is available (up). The default is `user account inactive`. **Notes** • If you do not specify a value for a parameter (the value is Null), the parameter always matches. To configure a parameter to never match, enter a "garbage" string that does not appear in the NDR. • If specifying a string for more than one Internet domain, the order in which you specify the keyword strings must correspond to the list of Internet domains. Separate more than one string with an "|"; do not use spaces.
NDR subject phrase identifying host is down	Provide a keyword string that should appear in the NDR subject when the host is not available. The default is unselected `route`. **Notes** • If you do not specify a value for a parameter (the value is Null), the parameter always matches. To configure a parameter to never match, enter a "garbage" string that does not appear in the NDR. • If specifying a string for more than one Internet domain, the order in which you specify the keyword strings must correspond to the list of Internet domains. Separate more than one string with an "|"; do not use spaces.
Data Collection	

Description	How To Set It
Collect data for connectivity (%)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of connectivity for the monitoring period. The default is unselected.
Event Notification	
Raise event if SMTP connectivity is down?	Select **Yes** to raise an event if SMTP connectivity is down. The default is Yes.
Event severity level when SMTP connectivity is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which SMTP connectivity is down. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is otherwise unavailable. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

TaskAvailability

Use this Knowledge Script to monitor the status of Domino, third-party, or user add-in tasks. This script raises an event when a task is down or when a task is up.

Resource Object

Domino server

Default Schedule

The default interval is **every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Monitor Administration Process (AdminP)?	Select **Yes** to monitor the AdminP task. The default is unselected.
Monitor Agent Manager (AMgr)?	Select **Yes** to monitor the AMgr task. The default is unselected.
Monitor Billing (Billing)?	Select **Yes** to monitor the Billing task. The default is unselected.
Monitor Calendar Connector (Calconn)?	Select **Yes** to monitor the Calconn task. The default is unselected.
Monitor Cataloger (Catalog)?	Select **Yes** to monitor the Catalog task. The default is unselected.
Monitor Chronos (Chronos)?	Select **Yes** to monitor the Chronos task. The default is unselected.
Monitor Cluster Administration Process (Cladmin)?	Select **Yes** to monitor the Cladmin task. The default is unselected.
Monitor Cluster Database Directory Manager (Cldbdir)?	Select **Yes** to monitor the Cldbdir task. The default is unselected.
Monitor Cluster Replicator (Clrepl)?	Select **Yes** to monitor the Clrepl task. The default is unselected.
Monitor Database Compactor (Compact)?	Select **Yes** to monitor the Compact task. The default is unselected.
Monitor Database Fixup (Fixup)?	Select **Yes** to monitor the Fixup task. The default is unselected.
Monitor Designer (Design)?	Select **Yes** to monitor the Design task. The default is unselected.
Monitor DIIOP (DIIOP)?	Select **Yes** to monitor the DIIOP task. The default is unselected.
Monitor Directory Cataloger (Dircat)?	Select **Yes** to monitor the Dircat task. The default is unselected.
Monitor Domain Indexer (Domidx)?	Select **Yes** to monitor the Domidx task. The default is unselected.
Monitor Event Monitor (Event)?	Select **Yes** to monitor the Event task. The default is unselected.
Monitor HTTP Server (HTTP)?	Select **Yes** to monitor the HTTP task. The default is unselected.
Monitor IMAP Server (IMAP)?	Select **Yes** to monitor the IMAP task. The default is unselected.
Monitor Indexer (Update)?	Select **Yes** to monitor the Update task. The default is unselected.
Monitor ISpy (ISpy)?	Select **Yes** to monitor the ISpy task. The default is unselected.

Description	How To Set It
Monitor LDAP Server (LDAP)?	Select **Yes** to monitor the LDAP task. The default is unselected.
Monitor MTC (MTC)?	Select **Yes** to monitor the MTC task. The default is unselected.
Monitor NNTP Server (NNTP)?	Select **Yes** to monitor the NNTP task. The default is unselected.
Monitor Object Store Manager (Object)?	Select **Yes** to monitor the Object task. The default is unselected.
Monitor POP3 Server (POP3)?	Select **Yes** to monitor the POP3 task. The default is unselected.
Monitor Replicator (Replica)?	Select **Yes** to monitor the Replica task. The default is unselected.
Monitor Reporter (Report)?	Select **Yes** to monitor the Report task. The default is unselected.
Monitor Router (Router)?	Select **Yes** to monitor the Router task. The default is unselected.
Monitor Schedule Manager (Sched)?	Select **Yes** to monitor the Sched task. The default is unselected.
Monitor Statistic Collector (Collect)?	Select **Yes** to monitor the Collect task. The default is unselected.
Monitor Statistics (Statlog)?	Select **Yes** to monitor the Statlog task. The default is unselected.
Monitor Stats (Stats)?	Select **Yes** to monitor the Stats task. The default is unselected.
Monitor Web Retriever (Web)?	Select **Yes** to monitor the Web task. The default is unselected.

Third-party tasks to monitor	Specify the name of a third-party task you want to monitor and its corresponding `.exe` file name using the format `<task name>:<exe name>`. For example:
	`NetIQ:nnetiq.exe`
	To monitor more than one third-party task, use the symbol "|" (shift+backslash), without any spaces, to separate the task name and executable file name pairs. For example:
	`taskname1:exename1|taskname2:exename2`

Data Collection	
Collect data for instance and overall availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the availability of selected tasks for the monitoring period. The default is unselected.
Event Notification	
Event severity level when a monitored task is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored task is down. The default is 5.
Event severity level when a monitored task is up	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored task is up. The default is 15.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event event severity level when nnetiq task is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.

Description	How To Set It
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is otherwise unavailable. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.

TaskDown

Use this Knowledge Script to monitor the status of Domino tasks that were found during discovery. To monitor third-party and user add-in tasks, use the *Additional tasks to monitor* parameter. This script can automatically restart any Domino task, third-party task, or user add-in task that is down.

Resource Object

Domino task

Default Schedule

The default interval is **every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Additional tasks to monitor	Provide the names of the third-party or user tasks you want monitor. Specify multiple tasks using the following format: `task1:display name1|task2:display name2` You can look up task names and display names using the `ShowTask` command in the Domino Console.
Data Collection	
Collect data for availability (%)?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of task availability for the monitoring period. The default is unselected.
Event Notification	
Raise event if task is down?	Select **Yes** to raise an event for each task that is down. The default is Yes.
Event severity level when auto-start is disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the *Auto-start task(s) if found down?* parameter is disabled. The default is 18.
Event severity level when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts a monitored task. The default is 25.
Event severity level when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart a monitored task. The default is 5.
Operations	
Auto-start tasks that are down?	Select **Yes** to automatically restart monitored tasks that are down. The default is Yes.
Data Acquisition Problems	

Description	How To Set It
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is otherwise unavailable. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

TopNAccessDbs

Use this Knowledge Script to monitor the top *n* Domino databases that are most frequently accessed on a Domino server. This script raises an event if the number of access requests exceeds the threshold you set.

The detail message includes the database name, the number of times the database was accessed, the database size, and the database whitespace for each top *n* database.

Resource Object

Domino server

Default Schedule

The default interval is **once every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Top “n” accessed databases to monitor	Specify the number of top databases you want to monitor. For example, to see the five databases that receive the most access requests, enter 5. The default is 10. Enter 0 to include all databases.
Number of previous hours to monitor	Specify the number of previous hours to monitor. The default is 24 hours.
Threshold - Maximum total requests during monitoring period	Specify the maximum number of access requests that can occur before an event is raised. The default is 1000 requests.
Data Collection	
Collect data for total access requests during monitoring period?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of access requests for the monitoring period. The default is unselected.
Event Notification	
Raise event if number of requests exceeds the threshold?	Select **Yes** to raise an event if the number of access requests exceeds the threshold you set. The default is Yes.
Event severity level when number of requests exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of access requests exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.

Description	How To Set It
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is otherwise unavailable. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

TopNDatabases

Use this Knowledge Script to monitor the Domino databases that use the most disk space on the Domino server. This script raises an event if the amount of disk space used by any database exceeds the threshold you set.

Resource Object

Domino database folder

Default Schedule

The default interval is **once every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Top “n” databases to monitor	Specify the number of top “n” largest databases you want to monitor. For example to see the five databases that use the most disk space, enter 5. The default is 10. Enter 0 to include all databases.
Threshold - Maximum total database disk space usage	Specify the maximum amount of disk space that can be used for all databases before an event is raised. The default is 50 MB.
Data Collection	
Collect data for total database disk space usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total amount of disk space used during the monitoring period. The default is unselected.
Event Notification	
Raise event if disk space usage exceeds threshold?	Select **Yes** to raise an event if the total amount of disk space usage exceeds the threshold you set. The default is Yes.
Event severity level when disk space usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of disk space usage exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.

Description	How To Set It
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is otherwise unavailable. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

TopNMailDatabases

Use this Knowledge Script to monitor the disk space used by the top *n* user mail files and mail-in databases on the Domino server. This script raises an event if the disk space used exceeds the threshold you set.

Resource Objects

Mail icon

Default Schedule

The default interval is **once every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Top “n” mail databases to monitor	Specify the number of top “n” largest mail files and mail-in databases you want to monitor. For example to see the five mail databases that use the most disk space, enter 5. The default is 10. Enter 0 to include all databases.
Threshold - Maximum total mail database disk space usage	Specify the maximum amount of disk space that can be used for all mail databases before an event is raised. The default is 50 MB.
Data Collection	
Collect data for total mail database disk space usage?	Select **Yes** to collect data for charts and reports. if enabled, data collection returns the amount of mail database disk space usage for the monitoring period. The default is unselected.
Event Notification	
Raise event if disk space usage exceeds threshold?	Select **Yes** to raise an event if the total amount of mail database disk space usage exceeds the threshold you set. The default is Yes.
Event severity level when disk space usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of mail database disk space usage exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.

Description	How To Set It
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is otherwise unavailable. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

TopNUnUsedDBs

Use this Knowledge Script to monitor the size of databases that are not being used. This script checks for databases that have not been accessed during the monitoring period. In addition, this script raises an event if the size of the unused databases exceeds the threshold you set.

Resource Object

Domino server

Default Schedule

The default interval is **once every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Top “n” least accessed databases to monitor	Specify the number of top unused databases you want to monitor. For example to see the five unused databases that use the most disk space, enter 5. The default is 10. Enter 0 to include all databases.
Number of previous hours to monitor	Specify the number of previous hours to monitor. The default is 24 hours.
Threshold - Maximum total database disk space usage	Specify the maximum amount of disk space that can be used by all unaccessed databases before an event is raised. The default is 1000 MB.
Data Collection	
Collect data for total database disk space usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of disk space used by unaccessed databases for the monitoring period. The default is unselected.
Event Notification	
Raise event if disk space usage exceeds threshold?	Select **Yes** to raise an event if disk space usage exceeds the threshold you set. The default is Yes.
Event severity level when disk space usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which disk space usage exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.

Description	How To Set It
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is otherwise unavailable. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

TopNUsers

Use this Knowledge Script to monitor the top *n* users that accessed the Domino server for the longest amount of time. This script raises an event when the number of minutes the top *n* users accessed the server exceeds the threshold you set. The detail message displays the combined number of minutes over the threshold for the top *n* users.

Resource Object

Domino server

Default Schedule

The default interval is **once every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Top “n” user access times to monitor	Specify the number of top users you want to monitor. For example to see the five users who access the Domino server most, enter 5. The default is 10 users. Enter 0 to include all users.
Previous hours to search (for Run Once)	Normally, this script monitors since the last interval. If you schedule the script to Run Once, enter the number of previous hours to search. The default is 24 hours.
Threshold - Maximum total user access time during monitoring period	Specify the maximum amount of time users can access the Domino server before an event is raised. The default is 50 minutes.
Data Collection	
Collect data for total users access time during monitoring period?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total number minutes users accessed the server during the monitoring period. The default is unselected.
Event Notification	
Raise event if total user access time exceeds threshold?	Select **Yes** to raise an event if the total user access time exceeds the threshold you set. The default is Yes.
Event severity level when user access time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which total user access time exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.

Description	How To Set It
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is otherwise unavailable. The default is 5.
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

UserSessions

Use this Knowledge Script to monitor the number of user sessions open on the Domino server. This script raises an event if the number of concurrent user sessions exceeds the threshold you set, which is an indication that the server is busy.

Resource Object

Domino server

Default Schedule

The default interval is **every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Monitoring	
Threshold - Maximum number of concurrent user sessions	Specify the maximum number of concurrent user sessions that can be open on the server before an event is raised. The default is 50 users.
Data Collection	
Collect data for concurrent number of user sessions?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of concurrent user sessions for the monitoring period. The default is unselected.
Event Notification	
Raise event if user sessions exceed threshold?	Select **Yes** to raise an event if the number of concurrent user sessions exceeds the threshold you set. The default is Yes.
Event severity level when user sessions exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of concurrent user sessions exceeds the threshold. The default is 5.
Data Acquisition Problems	
Raise event if nnetiq task unreachable?	Select **Yes** to raise an event if the nnetiq task is unavailable. Most monitoring data is gathered from this nnetiq task add-in to the Domino Server. Typically, the task is unavailable when the Domino Server is not running. Use ServerDown to monitor server status. The default is Yes.
Event severity level when nnetiq task unreachable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the nnetiq task is unavailable. The default is 25.
Raise event if data otherwise unavailable?	Select **Yes** to raise an event if the data is otherwise unavailable. Data can become unavailable because of a recent server restart, statistic values being reset, or data or other parsing errors. The default is Yes.
Event severity level when data otherwise unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data is otherwise unavailable. The default is 5.

Description	How To Set It
Collect data as '-1' for data unavailable?	Select **Yes** to log a -1 data point during an interval when a normal data point value could not be obtained. If Yes, the resulting data points show values AND points where data was unavailable. Note that "average" and "minimum" data values are subsequently skewed. If unselected, the resulting data points show only valid data values, and it may not be obvious when the Domino Server was down or data was otherwise unavailable. **Note** Function is applied to all Data Collection parameters. The default is unselected.
Threshold - Maximum wait time for server response	Specify the maximum number of seconds this script waits for a response from the Domino Server's nnetiq add-in task acknowledging a request for monitored data. This response time ensures that a "hung" Domino Server or nnetiq task will not "hang" this and other queued scripts. **Note** Setting the value too low may result in timeout events being generated unnecessarily. The default is 60 seconds.

Chapter 34
Exchange and Exchange2000 Knowledge Scripts

The Exchange and Exchange2000 categories provide the following Knowledge Scripts for monitoring Microsoft Exchange 2000 or Server 2003.

From the Knowledge Script view of Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. You can also click any Knowledge Script in the Knowledge Script pane of the Operator Console and press **F1**.

Knowledge Script	What It Does
CategorizerHealth	Monitors the health of Microsoft Message Categorizer.
CategorizerMessages	Monitors the message traffic of Microsoft Message Categorizer.
ClusterOwner	Determines the node ownership of an Exchange Virtual Server that is part of a cluster.
Connectivity	Monitors mail connectivity between Exchange servers.
ConnectorStatus	Monitors the up/down status of an Exchange connector.
DynSecsOldestMsgInMTAQueue	Reports how long, in seconds, the oldest message has been in the queue of MTA connections.
IMAP4Accesses	Monitors the total number of access operations for the IMAP4 server.
IMAP4Authenticate	Monitors the authentications of IMAP4 protocol stacks.
IMAP4Connections	Monitors the number of current IMAP4 connections and the total number of inbound and outbound connections.
InactiveMailboxes	Monitors the number of mailboxes that have not logged on to the Exchange server for a specified number of days.
InactivePublicFolders	Monitors the number of public folders that have not been accessed or modified for a specified number of days.
ISConnections	Monitors the number of information store connections.
ISLogFileSize	Monitors the size of Exchange log files in the MDBDATA and DSADATA directories on the Exchange server.
ISMailboxStoreAvgDlvryTime	Monitors mailbox store average delivery time to local recipients and storage providers.
ISMailboxStoreOpens	Monitors the rate of requests to the information store to open a mailbox store.
ISMailboxStoreSize	Monitors the disk space used by one or more mailbox stores.

Knowledge Script	What It Does
ISPubStoreAvgDeliveryTime	Monitors public store average delivery time to local recipients and storage providers.
ISPubStoreOpens	Monitors the rate of requests to the information store to open a public store.
ISPubStoreSize	Monitors the disk space used by one or more public stores.
LinkStatus	Monitors the status of all link queues for all X.400 and SMTP virtual servers, including the number, size, and elapsed time that messages reside in a link queue.
LogParser	Parses and queries a specified Exchange log file.
MailboxesOverStorageLimit	Monitors the number of mailboxes over the storage limit.
MailboxesWithoutStorageLimit	Monitors the number of mailboxes with no storage limitations.
MailboxStoreMountStatus	Monitors the mount status of one or more mailbox stores.
MsgAvgLocalDlvryTimeByIntrv	Monitors the average delivery time for local messages since the last time this script ran.
MsgsAvgLocalDeliveryTime	Monitors the average delivery time for local messages for specified days.
MsgsBetweenAdminGroups	Monitors the total number and size of messages transferred between Exchange Admin Groups during the specified number of days or from a specific start date to a specific end date.
MsgsBtwnAdmnGrpsByInterval	Monitors the total number and size of messages sent to an Admin Group or received from an admin group since the last time the Knowledge Script ran.
MsgsByServer	Monitors the number and size of messages transferred between a target Exchange server and all connected servers during the specified number of days or from a specific start date to a specific end date.
MsgsByServerByInterval	Monitors the number and size of messages transferred between a target Exchange server and all connected servers during the monitoring interval.
MsgsBySize	Monitors the number of messages in different size ranges over a specified number of days.
MsgsOfSystem	Monitors the load of directory and public folder replication messages between Exchange sites or Admin Groups.
MsgsOpenedByOWA	Monitors the number of messages opened by Outlook Web Access (OWA).
MsgsSentByOWA	Monitors the number of messages sent by Outlook Web Access (OWA).
MsgsSpecificDomainByInterval	Monitors the total number and size of messages transferred through an Internet Mail Connector (IMC) or SMTP service to and from a specific domain during the monitoring interval (delta value).
MsgsSpecificDomain	Monitors the total number and size of messages transferred through an Internet Mail Connector (IMC) or SMTP service to and from a specific domain during the specified number of days or from a specific start date to a specific end date.
MsgsThroughConnector	Monitors the total number and size of messages sent and received by one or more specified connectors on an Exchange site or routing group.

Knowledge Script	What It Does
MsgsThroughSMTPService	Monitors SMTP messages for the past N days or a range of days.
MsgsThruSMTPSvcByInterval	Monitors SMTP messages since the last time this script ran.
MsgsWithinAdminGroup	Monitors the total number and size of messages transferred between Exchange servers in the same Admin Group during the specified number of days or from a specific start date to a specific end date.
MsgsWthnAdmnGrpByInterval	Monitors the total number and size of messages transferred between Exchange servers in the same Admin Group since last time the Knowledge Script ran (a delta value).
MTAConnectionQueueLength	Monitors the queue length of all message transfer agent (MTA) connections.
NNTPConnections	Monitors connections to the Network News Transfer Protocol (NNTP) service.
NumberOfMailboxes	Monitors the total number of Exchange mailboxes.
PFAclChanges	Checks for changes in the access control lists for each folder in the public information store.
PFAclInfo	Monitors the access control list for each folder in the public information store.
PFInfo	Monitors the number and size of public folders, and the number of messages in the public folders.
PFReplicationByObj	Monitors public folder replication between Exchange servers by updating a test object.
POP3Accesses	Monitors the number of POP3 access operations.
POP3Authenticate	Monitors the authentications of POP3 protocol stacks.
POP3Connections	Monitors the number of current and total connections of POP3 service.
ProtocolVSStatus	Monitors the status of Exchange virtual servers.
PublicStoreMountStatus	Monitors the mount status of one or more public stores.
QueueStatus	Monitors the inbound and outbound message queue status of all X.400 and SMTP virtual servers, including the number, size, and elapsed time that messages reside in a message queue.
Report_Connectivity	Generates a report about the connectivity between Exchange servers.
Report_ISPrivateResourceSummary	Generates a report about the file space used by private information store folders and mailboxes.
Report_ISPublicResourceSummary	Generates a report about the file space used by public information store folders.
Report_ServerLoad	Generates a report about the rate at which messages are being sent and received and the rate at which RPC packets are being processed.
Report_ServerMessage	Generates a report about the total number of mail recipients, messages delivered, messages sent, messages submitted, and messages waiting to be delivered to the mailbox store and the public information stores.
Report_ServerUsers	Generates a report about the number of users connected to the information store.

Knowledge Script	What It Does
Report_TopNMailboxesInfo	Generates a report about the file space (in MB) used by the top private information store folders or mailboxes.
Report_TopNReceivers	Generates a report about which users received the most mail messages, and the total file size of messages received by the top users or by all users.
Report_TopNSenders	Generates a report about which users sent the most mail messages, and the total file size of messages sent by the top users or by all users.
ResponseTime	Checks the mail response time between Exchange servers.
ServerHealth	Monitors the percentage of time that all processors on the Exchange Server are busy and the percentage of elapsed time that the Exchange server process threads are used to execute instructions.
ServerHistory	Monitors the combined message count for the mailbox information and public information stores.
ServerLoad	Monitors the rate at which messages are being received and submitted per minute on the Exchange server.
ServerQueues	Monitors Exchange server queues, including the MTA work queue and the IS Private and the IS Public send and receive queues.
ServerTotalMsg	Monitors the total number of messages for an Exchange server.
ServerUsers	Monitors the number of users connected to the information store.
ServicesDown	Monitors the up and down status of Exchange services.
SMTPConnectivity	Verifies connectivity between an Exchange Server and one or more Internet domains by sending a message to a non-existent account and examining the non-delivery report (NDR).
SMTPConnectivityEx	Verifies connectivity between an Exchange Server and one or more Internet domains by examining the delivery report (DR) or the non-delivery report (NDR).
SRSServiceDown	Monitors the up and down status of the Site Replication Service.
TopNISMailboxRes	Monitors the file space used by the top private information store folders or mailboxes.
TopNISPublicRes	Monitors the file space used by the top public information store folders (public folders).
TopNReceivers	Monitors the total file size of mail messages received by the top users or all users.
TopNSenders	Monitors the total file size of mail messages sent by the top users or all users.

CategorizerHealth

Use this Knowledge Script to monitor the health of Microsoft Message Categorizer, including the rate of:

- Address book lookup completions processed per second
- Address lookups dispatched to Active Directory per second
- Categorization completions per second
- LDAP search completions processed per second
- LDAP searches successfully dispatched per second
- Messages being submitted to the Message Categorizer per second

This script raises an event if a monitored value exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003 SMTP Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the rate of: • Address book lookup completions processed per second • Address lookups dispatched to Active Directory per second • Categorization completions per second • Lightweight Directory Access Protocol (LDAP) search completions processed per second • LDAP searches successfully dispatched per second • Messages being submitted to the Message Categorizer per second The default is n.
Maximum threshold for the number of address lookup completions processed per second	Specify the maximum number of address lookup completions that can be processed per second before an event is raised. The default is 500.
Maximum threshold for the number of address lookups dispatched to the DS per second	Specify the maximum number of address lookups that can be dispatched to the Directory Service (DS) per second before an event is raised. The default is 500.
Maximum threshold for the rate of categorizations completed	Specify the maximum number of categorizations that can be completed per second before an event is raised. The default is 500.
Maximum threshold for the rate of LDAP search completions processed/sec	Specify the maximum number of LDAP search completions that can be processed per second before an event is raised. The default is 500.

Description	How to Set It
Maximum threshold for the rate of LDAP searches successfully dispatched/sec	Specify the maximum number of LDAP searches that can be successfully dispatched per second before an event is raised. The default is 500.
Maximum threshold for the rate that messages are being submitted to the categorizer	Specify the maximum number of messages per second that can be submitted to the Message Categorizer before an event is raised. The default is 500.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

CategorizerMessages

Use this Knowledge Script to monitor the message traffic of Microsoft Message Categorizer, including the number of messages in the following categories:

- Aborted during the monitoring interval
- Bifurcated during the monitoring interval
- Categorized during the monitoring interval
- Submitted during the monitoring interval
- In the Message Categorizer queue

This script raises an event if the number of messages in a category exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003 SMTP Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of messages in a category exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of messages: • Aborted during the monitoring interval • Bifurcated during the monitoring interval • Categorized during the monitoring interval • Submitted during the monitoring interval • In the Message Categorizer queue The default is n.
Maximum threshold for the number of messages marked to be aborted by the categorizer	Specify the maximum number of messages that can be marked to be aborted before an event is raised. The default is 200.
Maximum threshold for the number of new messages created by the categorizer (bifurcation)	Specify the maximum number of new messages that can be created by the Message Categorizer (bifurcation) before an event is raised. The default is 200.
Maximum threshold for the number of messages categorizer has submitted to queueing	Specify the maximum number of messages that can be submitted to queueing before an event is raised. The default is 200.
Maximum threshold for the number of messages submitted to the categorizer	Specify the maximum number of messages that can be submitted to the Message Categorizer before an event is raised. The default is 200.

Description	How to Set It
Maximum threshold for the number of messages in the categorizer queue	Specify the maximum number of messages that can be in the Message Categorizer queue before an event is raised. The default is 200.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number of messages in a category exceeds the threshold you set. The default is 5 (red event indicator).

ClusterOwner

Use this Knowledge Script to determine whether an Exchange Server computer that is part of a cluster is the owner of the node. This script raises an event if the computer is not the current node owner. In addition, this script generates data streams for ownership status.

Resource Object

Microsoft Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval for this script is Every 5 minutes

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if not node owner? (y/n)	Set to **y** to raise an event if the selected computer is in a cluster but is not the node owner. The default is n.
Collect data for ownership status? (y/n)	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following: • 100 - the computer is a cluster owner or the computer is not in a cluster • 0 - the computer is in a cluster but is not the cluster owner. The default is y.
Event severity when not node owner	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the selected computer is not the node owner. The default is 20.
Raise event when node is down? (y/n)	Set to **y** to raise an event if the selected node is down. The default is y.
Severity when the node is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the elected node is down. The default is 5.
Raise event when EVS is down? (y/n)	Set to **y** to raise an event if the selected EVS is down. The default is y.
Severity when the EVS is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the elected EVS is down. The default is 5.

Connectivity

Use this Knowledge Script to monitor mail connectivity between two or more Exchange 2000 or 2003 servers. This script cannot monitor more than one Exchange 2000 or 2003 virtual server.

This script determines whether e-mail can be delivered between Exchange servers and can help you diagnose mail delivery problems, such as problems with network connectivity, Exchange configuration, or Exchange services.

To monitor connectivity for a single Exchange server, use the AppManager ResponseTime for Microsoft Exchange module.

To test complete connectivity between Exchange servers in a non-cluster environment, run this script on the top-level Exchange folder in the Operator Console TreeView. Doing this causes the job to run on all Exchange servers and test each server's connection to the other servers and to itself, verifying complete connectivity between all Exchange servers.

You can also use this script to test connectivity between one server and a list of specified servers. To run this script on a group of Exchange servers, each server must have the same profile name.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what the job was doing when the failover occurred.

Note

This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information about setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Microsoft Exchange 2000 Server or Exchange Server 2003, Exchange folder

Default Schedule

The default interval is **Every 15 minutes**. This interval is recommended if you are checking connectivity between Exchange servers in a connected network.

If your Exchange servers rely on a remote WAN or LAN service (such as RAS) or a dial-up modem that is not always connected, you can set up server group folders to separate Exchange servers into different groups, then set the schedule interval for this Knowledge Script to run on each folder based on each group's connection schedule.

For example, you can create one server group for your always-connected servers and a separate folder for offhours RAS connections. Further, you can create two sets of jobs with different schedules. The schedules can be frequent for your connected network and once a day for the remote access servers.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a reply to a test message is not received within the specified time interval. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns a value of 100 if the connection between Exchange Servers is up or a value of 0 if the connection is down. The script also returns the response time in seconds for each successful connection between Exchange Servers and the time the connection was attempted. The default is y.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in the AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager. This is especially true if you are running this script as recommended on the top-level Exchange folder or Exchange server groups.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in the AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager. This is especially true if you are running this script as recommended on the top-level Exchange folder or Exchange server groups.

List of remote servers to monitor	Specify the computer names, separated by commas using the following syntax to check connectivity between specific Exchange 2000 or 2003 servers:
	`<computer>(/O=<organization>/OU=<administrative group>)`
	Where:
	• ***computer*** specifies the name of the computer on which the Exchange server is installed
	• ***organization*** specifies the name of the Exchange organization to which the server belongs
	• ***administrative group*** specifies the name of the Exchange administrative group to which the server belongs
	Separate multiple server names with commas, for example:
	`2K3Server(/O=org/OU=site1),2KServer(/O=Org2/OU=AdminGrp2)`
	This parameter allows you to run this script on a specific Exchange server and check connectivity with other specified servers (1*N). If you leave this field blank, this script checks the connectivity for all servers included in the scope of the job (N*N).

Maximum threshold for a response (in seconds)	Specify the maximum number of seconds that can elapse from the time the test message is sent out until a reply is received. If a reply to the test message is not received within this interval, it is not considered a valid reply. This script raises an event if the threshold is exceeded. The default is 120 seconds.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the response time threshold is exceeded. The default is 5 (red event indicator).

Example of How this Script Is Used

To test connectivity, this script sends a test mail message to each of the Exchange Servers being tested, using the specific account set up for the computer running the job. If the test message is not delivered, the script raises an event to indicate that the server cannot send mail. If the test message delivered by the sending server does not get a reply from each of the receiving servers, the script raises an event indicating the connection with the servers that failed to reply is down. If the test message is delivered but the reply is not received within an acceptable response time, the script raises an event indicating the response time with the server is above the threshold.

Checking Connectivity for Multiple Servers

The AppManager agent uses a mailbox on the local Exchange server where it resides. When you start the script job, the AppManager agent on each server sends a message from its mailbox to each of the other Exchange servers to which you are testing connectivity. Each of the receiving Exchange servers sees the message, and responds back with delivery confirmation.

At the next monitoring interval, the Connectivity job checks to see if the local Exchange server has received mail from the remote servers yet. If a reply has been received, there is connectivity between the local and remote servers. If a reply is not received, the connection is broken and an event is raised.

Assume you have four Exchange servers (a,b,c,d). Each of these servers has a default Exchange client profile and its own unique mailbox. If you run the Connectivity Knowledge Script on these four Exchange servers (a,b,c,d) in the TreeView, the management server starts a job on each of these servers to test connectivity to the other servers and itself, which is essentially a client-to-server connectivity test.

- The job of Exchange server **a** tests connectivity to a,b,c,d
- The job of Exchange server **b** tests connectivity to a,b,c,d
- The job of Exchange server **c** tests connectivity to a,b,c,d
- The job of Exchange server **d** tests connectivity to a,b,c,d

Only Exchange servers on which you run the Connectivity Knowledge Script are included in the connectivity test.

Because connectivity is always tested server to server, it does not matter if the servers are in the same site or different sites. When you create the Connectivity job, you need to include all the servers you want tested in the scope of the job. However, you can use server groups to organize your Exchange servers into sites or use the top level Exchange folder to test connectivity across all sites depending on the range of connectivity testing you want to do. You can also de-select a server you do not want to include in a test using the Objects tab in the Knowledge Script Properties dialog box.

To illustrate these principles, consider an Exchange environment with five Exchange servers: Paris, Cabernet, Dynamo, Boston, and Nero. Each of these servers has a special Windows user account that (1) the `NetIQ Corporationmc` service runs as on that server, and (2) has an Exchange profile and associated mailbox for sending and receiving mail.

If you only run the Connectivity Knowledge Script on the server Paris and do not specify any Exchange servers in the Remote server list, the **netiq-Paris Exchange client** sends a test message from its own mailbox to the **Exchange server Paris** and receives a confirmation when the delivery is successful.

If you run the Connectivity Knowledge Script on the server group, or top level folder that includes Paris and the four other Exchange servers, each server sends a test message to itself and to each of the other Exchange servers in the group. When a delivery confirmation message is received back at each sending server's mailbox within a reasonable period of time, the delivery was successful and connectivity is verified.

An Exchange profile must be associated with a Windows user account such as the `netiq_nt` user account. Although not required for this Knowledge Script, this user should generally be part of the Administrators group if you run other Knowledge Scripts such as ServicesDown to give the user account read, write, and execute permissions on the managed computer.

The Windows user account also needs Exchange Administrator privileges for permission to access to Exchange statistics, an Exchange profile (`netiq-Paris`), and a Mailbox alias (`netiq-Paris`) for sending and receiving mail.

The **mailbox alias** that the agent service `NetIQ Corporationmc` uses should be **unique** for each server. That is, each Exchange Server needs a unique mailbox alias for AppManager to use. Having separate mailboxes that physically reside on each server provides the best coverage for testing connectivity. In addition, using the `netiq-<computer_name>` convention for profiles and mailbox aliases helps you to verify that the test message is delivered to the proper recipients.

During installation, AppManager provides options for automatically creating and configuring profiles and mailbox aliases. If you select this option, the profiles and mailbox aliases are created and checked into the repository for you.

AppManager creates profiles and mailboxes for you even if you do not specify this option, but the information is not stored in the AppManager repository. You can use AppManager Security Manager to add the profile and mailbox names for each Exchange server after installation. You can also use AppManager Security Manager to update the AppManager repository when you change or manually create Exchange profiles and mailboxes.

Checking Connectivity from One Server to a Specified List

In addition to checking complete connectivity, a many-to-many relationship, you can use this Knowledge Script to check connections from a single Exchange server to a specified list of other Exchange servers. For example, assume you have the Exchange server **Paris** at your corporate headquarters. You may only be interested in checking its connectivity to the satellite Exchange servers **Dynamo** and **Cabernet** and not those servers' connectivity to each other.

To do this, you can run this Knowledge Script on Paris and specify `Dynamo,Cabernet` for the `Remote server list` parameter. The job then tests connectivity between Paris and Dynamo and Paris and Cabernet.

Interpreting Response Time Data

If you use this Knowledge Script to collect response time data for graphs and reports, you may notice a saw-tooth pattern of response times.

The peaks and valleys represent the response times found at each interval. The times along the bottom of the graph represent each time the Knowledge Script job ran and collected data.

This saw-tooth pattern is caused by a conflict between the interval set for running this Knowledge Script and a polling mechanism used internally by Exchange Server. Because Exchange is checking and responding internally to the test e-mail message **between job intervals**, the response times returned by the Knowledge Script become skewed.

To avoid this problem, set the interval for this Knowledge Script to some multiple of 56 seconds, for example, 112 and 224 seconds. Using an interval that synchronizes (as much as possible) the Knowledge Script job and the internal mechanism gives you a more consistent and realistic view of the server's response time.

Note
If your primary interest is monitoring the response time between Exchange servers, you may want to use the ResponseTime Knowledge Script rather than the Connectivityowledge Script.

Performing Periodic Maintenance

Periodically log in to each Exchange server using the same Windows account set up for the `NetIQ Corporationmc` service to do some housekeeping. For example, periodically remove old mail messages (that are at least a couple of days old) from the **Inbox,** and permanently remove deleted mail from the **Deleted Item** box. Depending on how frequently you run this script, consider performing these activities weekly or monthly.

ConnectorStatus

Use this Knowledge Script to monitor the status of an Exchange 2000 or 2003 connector. This script raises an event if the connector is detected as down.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a connector is down. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns 100 if the monitored connector is up, 0 if the connector is down. The default is n.
List of connectors to monitor (comma separated)	Specify the names of the connectors you want to monitor, separating multiple names with commas, or specify **ALL** to monitor all connectors on the computer. The default is ALL.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a connector is down. The default is 5 (red event indicator).

DynSecsOldestMsgInMTAQueue

Use this Knowledge Script to identify the ages, in seconds, of messages in MTA queues that exceed a specified threshold.

Resource Object

MTA Queue folder, if dynamically enumerating connections. If you are not enumerating connections dynamically, you can run this script on the MTA Queue folder or on individual queue objects, such as DS Queue, IMC Queue, Public IS Queue, Private IS Queue, Machine Queue, X400 Queue, MSMail Queue, and Directory Queue.

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Create event if old messages are found in a queue?	Set to **Yes** to raise an event if the age of messages in the MTA queue exceeds the threshold you set. The default is Yes.
Severity - Old messages found in queue	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the age of messages in the queue exceeds the threshold. The default is 15 (Yellow event indicator).
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DynSecsOldestMsgInMTAQueue job fails. The default is 5 (red event indicator).
Data Collection	
Collect message age data?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the age of messages in the queue. The default is unchecked.
Monitoring	
Dynamically enumerate MTA queues	Set to **Yes** to enable dynamic enumeration of MTA queues. The default is Yes.
MTA queue exclude list	If needed, specify a comma-separated list of MTA queues that should not be monitored. For example: `microsoft public mdb,microsoft private mdb`.
Threshold - Age of messages in the queue	Specify the maximum age that messages in the queue can attain before an event is raised. The default is 1440 seconds.

IMAP4Accesses

Use this Knowledge Script to monitor the number of IMAP4 access operations. Access operations include `SELECT`, `EXAMINE`, `APPEND`, `SUBSCRIBE`, `UNSUBSCRIBE`, `LIST` and `SUB` operations. This script raises an event if the total number of IMAP4 access operations exceeds the threshold you specify.

Resource Object

IMAP4 Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of operations exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of IMAP4 access operations. The default is n.
Maximum threshold for number of IMAP4 access operations	Specify the maximum number of IMAP4 access operations that can occur before an event is raised. The default is 10000 access operations.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number of operations exceeds the threshold. The default is 5 (red event indicator).

IMAP4Authenticate

Use this Knowledge Script to monitor the authentication of IMAP4 protocols. This script raises an event if the rate of failure of total authentications exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003, Protocols folder

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of authentication failures exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Number of authenticate commands received since startup • Number of authenticate commands per second • Number of authenticate command failures since startup The default is n.
Maximum threshold for number of authentication failures	Specify the maximum number of authentication failures that can occur before an event is raised. The default is 1000.
Consecutive number of times before an event	Specify the maximum number of consecutive times the threshold can be exceeded before this script raises an event. The default is 5 consecutive occurrences.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number of authentication failures exceeds the threshold. The default is 5 (red event indicator).

IMAP4Connections

Use this Knowledge Script to monitor the number of current IMAP4 connections and the total number of inbound and outbound IMAP4 connections since the IMAP4 service started. This script raises an event if the number of current or total connections exceeds the threshold you set.

Resource Object

IMAP4 Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default option is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Current connections • Total connections The default option is n.
Maximum threshold for current connections	Specify the maximum number of current IMAP4 connections that can occur before an event is raised. The default is 100 current connections.
Maximum threshold for total connections	Specify the maximum number of IMAP4 connections that can occur before an event is raised. The default is 1000 connections.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

InactiveMailboxes

Use this Knowledge Script to monitor the number of inactive Exchange mailboxes. An inactive mailbox is a mailbox that has not logged on to the Exchange server for a specified number of days. This script raises an event if the number of inactive mailboxes exceeds the threshold you set.

On a computer with more than one virtual server, the total number of inactive mailboxes is calculated as the total number of inactive mailboxes for all virtual servers on the computer.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information about setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Microsoft Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of inactive mailboxes exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of inactive mailboxes. The default is n.
Inactive after N days	Specify the number of days to use as a measure of whether a mailbox is inactive. The default is 10 days.
Maximum threshold for number of inactive mailboxes	Specify the maximum number of mailboxes that can be inactive before an event is raised. The default is 300 inactive mailboxes.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of inactive mailboxes exceeds the threshold. The default is 5 (red event indicator).

InactivePublicFolders

Use this Knowledge Script to monitor the number of inactive Exchange public folders. An inactive folder is a public folder that has not been accessed or modified for a specified number of days. This script raises an event if the number of inactive public folders exceeds the threshold you set.

This script helps you manage infrequently accessed information resources that can, over time, consume valuable resources.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information about setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Microsoft Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of inactive public folders exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of inactive public folders. The default is n.
Inactive after N days	Specify the number of days to use as a measure of whether a public folder is inactive. The default is 10 days.
Maximum threshold for number of inactive folders	Specify the maximum number of public folders that can be inactive before an event is raised. The default is 300 inactive public folders.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of inactive public folders exceeds the threshold.The default is 5 (red event indicator).

ISConnections

Use this Knowledge Script to monitor both the number of active connections and the total number of connections to the information store. This script raises an event if the number of either the active or the total connections is over the threshold for the specified consecutive number of intervals.

Resource Object

Information Store folder

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Total connections • Active connections The default is n.
Maximum threshold for total number of connections	Specify the maximum total number of connections to the information store that can occur before an event is raised. The default is 100 connections.
Maximum threshold for number of active connections	Specify the maximum number of information store connections that can be active before an event is raised. The default is 100 connections.
Consecutive number of times before an event	Specify the consecutive number of intervals during which the threshold for connections can be exceeded before the script raises an event. The default value is 5 consecutive intervals. Because connections can have periodic spikes, you can set this parameter to a higher value to filter out unnecessary events. For example, you can allow the number of active connections to exceed the threshold 3 to 4 times before an event is raised.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ISLogFileSize

Use this Knowledge Script to monitor the size of transaction logs and the reserved transaction log files on Exchange 2000 Server or Exchange Server 2003. This script raises an event if the size of the transaction logs exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the size of the transaction logs exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the log file size in MB. The default is n.
Maximum threshold for log file size (MB)	Specify the maximum size the transaction logs can attain before an event is raised. The default is 400 MB.
Logs you want to monitor	Specify one of the following values to specify the log you want: • **EDB** specifies transaction log. • **RES** specifies reserved transaction log. • **ALL** specifies both logs listed above. The default, ALL, monitors all logs for the Exchange version.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the size of the transaction logs exceeds the threshold. The default is 5 (red event indicator).

ISMailboxStoreAvgDlvryTime

Use this Knowledge Script to monitor the average time between the submission of a message to a mailbox store and the subsequent delivery of the message to local recipients (on the same server) or to other storage providers. This script reports the average delivery time for the last ten messages. This script raises an event if the average delivery time to local recipients or other storage providers exceeds the thresholds you set.

This script helps you manage the performance of mailbox stores.

Resource Object

Information Store folder, Mailbox Store object

Default Schedule

The default interval is **Every 3600 seconds**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the average delivery time to other storage providers, and the average local delivery time for the mailbox store. The default is n.
Maximum threshold for the rate at which messages are delivered locally	Specify the maximum rate at which messages can be delivered locally before an event is raised. The default is 500 deliveries per second.
Maximum threshold for the rate that requests to open folders are submitted to the information store.	Specify the maximum rate at which requests to open folders can be submitted before an event is raised. The default is 500 submissions per second.
Maximum threshold for the rate that requests to open messages are submitted to the information store.	Specify the maximum rate at which requests to open messages can be submitted before an event is raised. The default is 500 submissions per second.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ISMailboxStoreOpens

Use this Knowledge Script to monitor the number of requests per second submitted to the information store to open a mailbox store. If the rate of requests to open a mailbox store increases, it may indicate increased demand on the Exchange 2000 server or increased user activity. This script raises an event if the number of requests per second exceeds the threshold you set.

Resource Object

Information Store folder, Mailbox Store object

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of mailbox open requests received per second. The default is n.
Maximum threshold for number of folder requests	Specify the maximum rate at which folder requests can be submitted before an event is raised. The default is 100 requests per second.
Maximum threshold for number of message requests	Specify the maximum rate at which message requests can be submitted before an event is raised. The default is 100 requests per second.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ISMailboxStoreSize

Use this Knowledge Script to monitor the disk space used by a mailbox store. This script raises an event if the size of a monitored mailbox store, a Microsoft Access Database (MDB) file, exceeds the threshold you set.

Resource Object

Information Store folder, Mailbox Store object

Default Schedule

The default interval is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the size of a mailbox store exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the file size, in megabytes, of the specified mailbox store. The default is n.
Maximum threshold for size of mailbox store (MB)	Specify the maximum size a mailbox store can attain before an event is raised. The default is 4000 MB.
MDB files to monitor (EDB, Stream, or ALL)	Specify the mailbox store files you want to monitor: • **EDB** monitors regular message data. • **Stream** monitors streaming message data. • **ALL** monitors regular and streaming message data. The default is ALL.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the size of mailbox store exceeds the threshold. The default is 5 (red event indicator).

ISPubStoreAvgDeliveryTime

Use this Knowledge Script to monitor the average time between the submission of a message to a public store and the subsequent delivery of the message to local recipients (on the same server) or other storage providers. This script reports the average delivery time for the last ten messages. This script raises an event if the average delivery time to local recipients or other storage providers exceeds the thresholds you set.

This script helps you manage the performance of public stores.

Resource Object

Information Store folder, Public Store object

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the average local delivery time and the average delivery time to other providers for the public store. The default is n.
Maximum threshold for average delivery time to local recipients	Specify the maximum average delivery time to local recipients that can occur before an event is raised. The default is 500 seconds.
Maximum threshold for average delivery time to storage providers	Specify the average delivery time to other storage providers that can occur before an event is raised. The default is 500 seconds.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ISPubStoreOpens

Use this Knowledge Script to monitor the number of requests per second submitted to the information store to open a public store. If the rate of requests to open a public store increases, it may indicate increased demand on the Exchange 2000 server or increased user activity. This script raises an event if the number of requests per second exceeds the threshold you set.

Resource Object

Information Store folder, Public Store object

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of folders opened per second. The default is n.
Maximum threshold for number of folder requests	Specify the maximum rate at which requests to open folders can be submitted before an event is raised. The default is 100 requests per second.
Maximum threshold for number of message requests	Specify the maximum rate at which requests to open messages can be submitted before an event is raised. The default is 100 requests per second.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ISPubStoreSize

Use this Knowledge Script to monitor the disk space used by any public store in the TreeView. This script raises an event if a monitored public store, a Microsoft Access Database (MDB) file, exceeds the threshold you set.

Resource Object

Information Store folder, Public Store object

Default Schedule

The default interval is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the size of a public store exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the size, in megabytes, of the public store. The default is n.
Maximum threshold for size public store (MB)	Specify the maximum size a public store can attain before an event is raised. The default is 4000 MB.
MDB files you want to monitor (EDB, Stream, or ALL)	Specify the public store files you want to monitor: • **EDB** monitors regular message data. • **Stream** monitors streaming message data. • **ALL** monitors regular and streaming message data. The default is ALL.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the size of a public store exceeds the threshold. The default is 5 (red event indicator).

LinkStatus

Use this Knowledge Script to monitor the status of all link queues for all X.400 and SMTP virtual servers, including the number, size, and elapsed time for messages that reside in a link queue. This script monitors the link queue status at each monitoring interval and gives you a "snapshot" of the link queue status.

In Exchange 2000 or Exchange Server 2003, messages with the same next-destination server are transferred into the same queue. This queue is known as a *link queue*. Messages reside in the link queue until an active connection is made with the next-destination server, and that server agrees to process the messages.

Note
Although system queues are always visible, link queues may disappear after all messages have been sent to the next-destination server. The link queue will appear again when new messages are queued.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Once a day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Specify a protocol (X400, SMTP, or ALL)	Specify the protocol you want to monitor (not case-sensitive): • **X400** monitors the X.400 protocol. • **SMTP** monitors the SMTP protocol. • **ALL** monitors both X.400 and SMTP protocols. The default is ALL.
Collect total number of messages, link size and elapsed time of links?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of messages, link size, and elapsed time that messages reside in a link queue. The default is n. Use the parameters that follow to monitor or change the default event thresholds for the total number of messages, link size, or elapsed time that messages reside in a link queue.
Collect data for number of messages in links?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of messages in a link queue. The default is n.
Maximum threshold for number of messages in links	Specify the maximum number of messages that can be in a link queue before an event is raised. The default is 1000.
Event for number of messages in links?	Set to **y** to raise an event when the server exceeds the threshold for number of messages. The default is y.
Event severity: Number of messages in links	Set the event severity level, from 1 to 40, to specify the importance of an event in which the number of messages in the link queue exceeds the threshold. The default is 5 (red event indicator).

Description	How to Set It
Collect data for size of links?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the size of a link queue. The default is n.
Maximum threshold for size of links	Specify the maximum size a link queue can attain before an event is raised. The default is 100 MB.
Event for size of links?	Set to **y** to raise an event if the size of a link queue exceeds the threshold. The default is y.
Event severity: Size of links	Set the event severity level, from 1 to 40, to specify the importance of an event in which the size of a link queue exceeds the threshold. The default is 5 (red event indicator).
Collect data for elapsed time in links?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the oldest messages in a link queue. The default is n.
Maximum threshold for elapsed time in links	Specify the maximum amount of time that a message can remain in a link queue before an event is raised. The default is 1000 seconds.
Event for elapsed time in links?	Set to **y** to raise an event if a message exceeds the threshold for elapsed time in a link queue. The default is y.
Event severity: Elapsed time in links	Set the event severity level, from 1 to 40, to specify the importance of an event in which a message exceeds the threshold for elapsed time in a link queue. The default is 5 (red event indicator).

LogParser

Use this Knowledge Script to execute a query against Exchange log files and return those results in an event message or in a data stream. This script invokes Microsoft Log Parser, which uses Structured Query Language (SQL) to process Exchange log files. Microsoft Log Parser executes your query on the Exchange logs on the monitored Exchange server.

You build your query statement using Query Builder, which you access from the *Launch Query Builder* parameter on the Values tab. For more information, see "Using Query Builder" on page 1843.

This script raises an event if the number of matches to your query exceeds the threshold you set.

You can save the results of the query to a comma-separated values (.csv) file in a location you specify on the monitored Exchange server.

Prerequisite

Microsoft Log Parser version 2.2 installed on the monitored Exchange server and on each console computer where you will use Query Builder. You can download Microsoft Log Parser from the Microsoft Download Center.

Resource Object

Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval for this Knowledge Script is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Create event if matches are found?	Set to **Yes** to raise an event if the number of matches to your query exceeds the value you set for the *Threshold for matching lines* parameter. The default is Yes.
Severity - Matches found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of matches to your query exceeds the threshold you set. The default is 15.
Maximum number of records to display	Specify the maximum number of records to display in the event's Messages tab. If *Collect data?* is set to Yes, then this value also controls the number of records displayed in the data detail. The default is 25.
Threshold for matching lines	Specify the maximum number of matching lines that a query can return before an event is raised. The default is 0.
Create event if no matches are found?	Set to **Yes** to raise an event if no matches to your query are returned. The default is unchecked.

Description	How to Set It
Severity - No matches found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no matches to your query are returned. The default is 20.
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the LogParser job fails. The default is 5. **Note** Invalid SQL syntax in your query statement can cause the LogParser job to fail. The event detail message will identify the failure.
Data Collection	
Collect data?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns one data stream based on the parsed result set. The default is unchecked. Each data point in a data stream contains the number of matched rows for that iteration of the script. The data detail contains a list of the records that matched your query, based on the value you set in the *Maximum number of records to display* parameter.
Monitoring	
Query building process	Select the way you want to build your query in the Query Builder dialog box: • Select **Manual** to type your own SQL query statement in the Query Builder dialog box. • Select **Query tool** to use the interactive elements (such as lists and check boxes) of the Query Builder dialog box to build your SQL query statement. The default is Query tool.
Launch Query Builder	Click **Browse [...]** to open the Query Builder dialog box and build your query. For more information, see "Using Query Builder" on page 1843.
Scan entire file at each iteration?	Set to **Yes** to scan the entire log file at every iteration of the Knowledge Script job. The default is unchecked. If this option is not selected, the first iteration of the Knowledge Script job places a marker at the end of the log file. During a subsequent iteration, the script scans the log file from the marked point and processes new log entries only.
Save query results to a file?	Set to **Yes** to save the entire results of your query to a .csv file. Use the *Full path to results file* parameter to indicate where you want to save the results file. The default is unchecked.
Full path to results file	Specify the full path to the location in which you want to save the results .csv file. The default location is `C:\Program Files\NetIQ\Temp\`.

Using Query Builder

Query Builder is a component of the LogParser Knowledge Script that allows you to build complex SQL queries manually or with the help of the Query tool. Use Query Builder to construct your query before running LogParser.

Building a Query with the Query Tool

You can simplify the process of building a SQL query by choosing **Query tool** in the *Query building process* parameter in the LogParser Knowledge Script, and then clicking **Browse [...]** in the *Launch Query Builder* parameter.

Notes

- Microsoft Log Parser version 2.2 must be installed on the monitored Exchange server and on each console computer where you will use Query Builder.
- For examples of building a query with the Query tool, see "Using the Query Tool - Example 1" on page 1846 and "Using the Query Tool - Example 2" on page 1846.

To build a query using the Query tool in Query Builder:

1. Build your SQL query in Query Builder according to the field descriptions in the table below.
2. When you have finished building your query, click **OK**. Query Builder returns your query statement to the LogParser Knowledge Script.

Field	Description
Type of Log	Query Builder uses the W3C Log File format. You cannot change the selection.
Sample Log File	Click **Browse** to select a log file that is an *example* of the log file you want to query. You can use the built-in sample file, which ships with AppManager for Exchange 2000 or 2003 and is installed by default on your local system at `C:\Program Files\NetIQ\AppManager\bin\SampleExchLogFile.log`. Query Builder uses the column names in the sample log file to populate the contents of the Column List field.
Log File Path on Server	Specify the full path to the location of the Exchange log you want to query. This field is disabled when the **Auto Detect Log File Path** option is enabled. To manually specify a log location, you must first enable **Auto Detect Log File Path**. The path is displayed in the Query Statement section as the "From" statement in your query. For example: `From C:\program Files\exchsrvr\LabServer.log` **Tip** If you want to run the LogParser script on several Exchange servers, and the path to the Exchange log is the same for each server, you can use the `{Server Name}` variable in the file path. By default, the names of Exchange logs contain the name of the server. Therefore, when searching for your Exchange log, AppManager replaces the variable with the name of the server on which you run the LogParser script. For example, type `C:\Program Files\exchsrvr\{Server Name}.log`
Auto Detect Log File Path	This option is the preferred method for identifying the Exchange log to query. Select to automatically detect the location of the Exchange log on the monitored Exchange server. The LogParser Knowledge Script determines the Exchange log directory based on the configuration of the Exchange server. Your selection is displayed in the Query Statement field as the "From" statement in your query. For example: `From {Auto Detect}\*.log`
Column List	Contains a list of the columns in the sample log file. Select the columns that you want to use in your query. Your selections are displayed in the **Columns** field in the Criteria section and in the Query Statement field as the "Select" statement of your query. For example: `Select client-ip,Client-hostname,message-subject` For more information about what each column contains, see "Understanding Log File Columns" on page 1849.

Field	Description
Criteria	Use the fields in this section to customize your query. Your selections are displayed in the Query Statement section.
Show	Select to include the associated column in your query statement. Clear to remove the associated column from your query statement. Although the column is removed from the statement, it is not removed from the Criteria section.
Columns	This field is automatically populated by your selections in the **Column List** field. Your selections are displayed in the Query Statement section as the “Select” statement in your query. For example: `Select total-bytes` **Tip** You can click in a blank field in this column to select a column name to include in the query. This feature is helpful if you want to set multiple conditions on the same column: select the same column name in two or more fields and then customize each row for each separate set of query operators and keywords.
Group By	Allows you to perform aggregate functions, such as SUM, for selected column values, rather than for the entire column. Select the function you want to perform: • Sum • Count • Max • Min • Avg Your selection is displayed in the Query Statement section as part of the “Select” statement in your query. For example: `Select Avg(total-bytes)`
Rename To	Provide a new name for the column to display in the results. This feature allows you to display an alternative column name in the query results. The new name is displayed in the Query Statement section as part of the “Select” statement in your query. For example: `Select Avg(total-bytes) As Average Total Bytes`
Sort Type	Select **Ascending** or **Descending** to sort the results for the associated column name. Your selection is displayed in the Query Statement section as part of the “Order By” statement in your query. For example: `Order By Date Asc`
Grouping	Select to group query results by the associated column name. Your selection is displayed in the Query Statement section as part of the “Group By” statement in your query. For example: `Group By Date`
Operator	Select a method for filtering log entries based on one or more conditions. • **>** finds log entries that are greater than the specified condition. • **<** finds log entries that are less than the specified condition. • **=** finds log entries that match the specified condition. • **>=** finds log entries that are greater than or match the specified condition. • **<=** finds log entries that are less than or match the specified condition. • **NOT** finds log entries that *do not* match the specified condition. • **LIKE** allows you to use wildcards to find log entries for the specified condition. -- Use the % wildcard to match a text string of any length -- Use the _ wildcard to match a single character Your selection is displayed in the Query Statement section as part of the “Where” statement in your query. For example: `Where Date = 20080925`

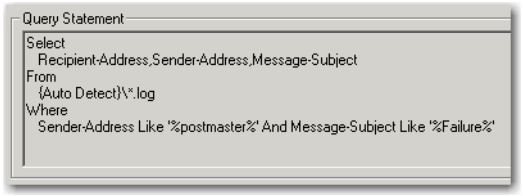
Field	Description
Condition	Type the value you want to compare for the associated column. Your selection is displayed in the Query Statement section as part of the "Where" statement in your query. For example: `Where Date = 20080925` If you selected **LIKE** in the **Operator** field, use the wildcard along with your value in the **Condition** field. **Note** If the associated column supports the "String" type, rather than an "Integer," a "Timestamp," or a "Real" type, enclose your condition text in single quotes, for example: `'production-server'`.
Remove	Click to remove the associated column from your query statement *and* from the Criteria section. This action also clears the column name in the **Column List** field.
Query Statement	As you select information in the fields in Query Builder, the Query Statement section reflects the selections you make in SQL query syntax. You cannot change information directly in the Query Statement section. Yyou must do so by changing your selections in the Criteria section. **Tip** If a query statement you build with Query Builder is not as complex as you need it to be, you can copy the contents of the Query Statement section and use the manual query option. From there, you can manually complete your query. For more information, see "Building a Query Manually" on page 1848.

Using the Query Tool - Example 1

In the following example, use the Query Tool to build a query that will look for Exchange log entries for which the recipient has received email messages that contain the word "Failure" in the message subject and were sent from the postmaster. Depending on your threshold and data collection selections, the LogParser Knowledge Script event message and data details return the column entries that match the conditions you set.

To build query example 1:

1. Accept the default values for the **Type of Log** and **Sample Log File** fields.
2. Select **Auto Detect Log File Path**.
3. In the **Column List** field, select **Recipient-Address**, **Sender-Address**, and **Message-Subject**.
4. In the **Operator** field for the Sender-Address column, select **LIKE**.
5. In the **Condition** field for the Sender-Address column, type `'%postmaster%'`.
6. In the **Operator** field for the Message-Subject column, select **LIKE**.
7. In the **Condition** field for the Message-Subject column, type `'%Failure%'`. The Query Statement field contains the following query statement:



8. Click **OK**.

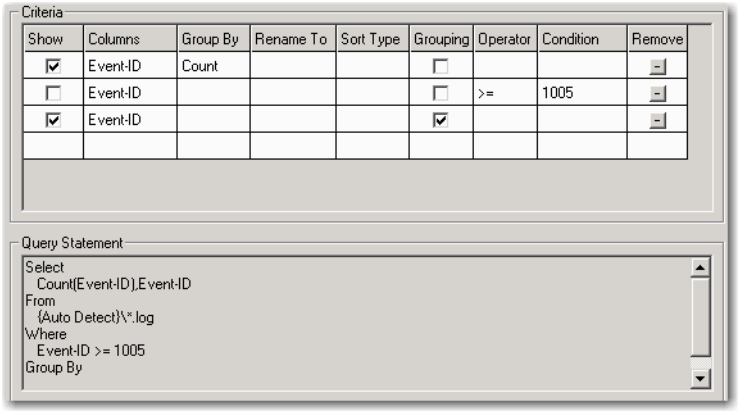
Using the Query Tool - Example 2

In the following example, you use the Query Tool to build a query that uses multiple instances of the same column.

The purpose of this query is to return a count of all Event ID values greater than or equal to 1005 and group them by Event ID value.

To build query example 2:

1. Accept the default values for the **Type of Log** and **Sample Log File** fields.
2. Select **Auto Detect Log File Path**.
3. In the **Column List** field, select **Event-ID**. A row for the Event-ID column is displayed in the **Criteria** field.
4. In the blank row below the Event-ID row, click in the **Columns** field and select **Event-ID** to create a second row for the Event-ID column.
5. Repeat step 4 to create a third row for the Event-ID column.
6. Note that for all rows, **Show** is selected. Clear **Show** for the second, or middle, row to remove it from the Select statement.
7. In the first row, select **Count** in the **Group By** field.
8. In the second row, the row for which **Show** is cleared, select **>=** (greater than or equal to) in the **Operator** field and type `1005` in the **Condition** field.
9. In the third row, select **Grouping**. Your completed query should look like this:



10. Click **OK**.

The LogParser Knowledge Script event message and data details return the count of Event-ID values greater than or equal to 1005 grouped by the Event-ID value, as illustrated in the following picture.

Log Parser Query Result

COUNT(ALL Event-ID)	Event-ID
831	1019
1097	1025
1097	1024
1097	1033
962	1034
133	1030
135	1036
135	1023
135	1028
132	1021
2	1027
652	1020
652	1031

Building a Query Manually

You can manually build a SQL query by choosing **Manual** in the *Query building process* parameter in the LogParser Knowledge Script, and then clicking **Browse [...]** in the *Launch Query Builder* parameter.

To build a query manually in Query Builder:

1. Build your query in Query Builder according to the field descriptions. If you do not have Microsoft Log Parser 2.2 installed, only the **Query Statement** field is displayed in the dialog box.

Field	Descriptions
Type of Log	Query Builder uses the W3C Log File format. You cannot change this selection.
Sample Log File	Click **Browse** to select a log file that is an *example* of the log file you actually want to query. You can use the built-in sample file, which ships with AppManager for Exchange 2000 or 2003 and is installed by default on your local system at `C:\Program Files\NetIQ\AppManager\bin\SampleExchLogFile.log`.
Column List	Contains a list of the columns in the sample log file. Refer to these column names when building your query statement. For more information about what each column contains, see "Understanding Log File Columns" on page 1849.
Query Statement	Using standard SQL query syntax, type your query statement. For more information, see "Building a Query Manually" on page 1848.

2. When you have finished building your query, click **OK**. Query Builder returns the query statement to the LogParser Knowledge Script.

Manually Building a Query - Example

The Query Builder Query tool does not support expressions such as "In." To use the "In" condition, you must manually build a query. The following example details the process of building a query that parses the Exchange log for specified Event IDs. The LogParser Knowledge Script event message and data details return the column entries that match the conditions you set.

To build the manual query example:

1. In the **Query Statement** field, type the following Select statement to identify the columns you want to include in your query.

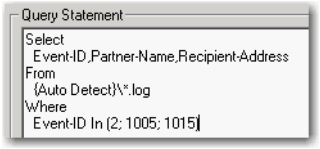
   ```
   Select Event-ID,Partner-Name,Recipient-Address
   ```

2. To enable AppManager to automatically find the Exchange log you want to parse, type `From {Auto Detect}\*.log`.

3. Type the following Where statement to identify the Event IDs you want to find in the Exchange log.

   ```
   Where Event-ID In (2; 1005; 1015)
   ```

   The completed query statement looks similar to the following:

4. Click **OK**.

Understanding Log File Columns

Use the information provided in this section to build queries for the LogParser Knowledge Script, which supports Exchange log file formats. The following table provides the Microsoft descriptions for the column names in Exchange log files:

Column Name	Type	Description
Date	STRING	The date of the event.
Time	STRING	The Greenwich mean time of the event.
client-ip	STRING	The IP of connecting client.
Client-hostname	STRING	The hostname of connecting client.
Partner-Name	STRING	The name of the messaging service that the message is handed off to. In Exchange 2000, the service can be: SMTP, X400, MAPI, IMAP4, POP3, STORE. This is essentially the same as Exchange Server 5.5, but in Exchange 2000, there are more possibilities for this field.
Server-hostname	STRING	The hostname of the server that makes the log entry.
server-IP	STRING	The IP address of the server that makes the log entry.
Recipient-Address	STRING	The message recipient (SMTP or X.400 address).
EventID	INTEGER	An integer value corresponding to the Event Type of the logged actions such as sent, received, delete, retrieve.
MSGID	INTEGER	The message ID.
Priority	INTEGER	The priority level, represented by -1 if low, 0 if normal, 1 if high.
Recipient-Report-Status	INTEGER	A number representing the result of an attempt to deliver a report to the recipient: 0 if delivered, 1 if not delivered. This is used only for non-delivery reports (NDRs) and delivery reports (DRs). On other events, it is blank.
total-bytes	INTEGER	The message size in bytes.
Number-Recipients	INTEGER	The total number of recipients.
Origination-Time	STRING	The delivery time (in seconds) representing the time it takes to deliver the message. This is determined from the difference between the timestamp and time encoded in Message ID. This is only valid for messages within the Exchange organization (all versions). There is no requirement to decode other product message IDs such as Sendmail.
Encryption	INTEGER	The encryption level (For the primary body part: 0 if there is no encryption, 1 if signed, 2 if encrypted. This is per message, not per recipient).
service-Version	STRING	The version of the service making the log entry.
Linked-MSGID	STRING	If there is a MSGID from another service, it is given here to link the message across services.
Message-Subject	STRING	The subject of the message, truncated to 256 bytes.
Sender-Address	STRING	The primary address of the originating mailbox, if known. This could be SMTP, X.400, or Distinguished Name (DN), depending on the transport.

MailboxesOverStorageLimit

Use this Knowledge Script to monitor the number of mailboxes over the storage limit. This script provides useful report data to help you manage Exchange mailboxes.

On a computer with more than one virtual server, the total number of mailboxes over the storage limit is calculated as the total number of mailboxes over the storage limit for all virtual servers on the computer.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of mailboxes over the storage limit exceed the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of mailboxes that exceed the storage limit. The default is n.
Maximum threshold for number of mailboxes	Specify the maximum number of mailboxes that can exceed their storage limit before an event is raised. The default is 300 mailboxes.
Exchange profile for NetIQ Corporationmc log on as account	Enter a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Mailbox alias for NetIQ Corporationmc log on as account	Enter a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

MailboxesWithoutStorageLimit

Use this Knowledge Script to monitor the number of mailboxes with no storage limitation. This script provides useful report data to help you manage Exchange mailboxes.

On a computer with more than one virtual server, the total number of mailboxes without a storage limit is calculated as the total number of mailboxes without a storage limit for all virtual servers on the computer.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

Note

This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of mailboxes with no storage limitation exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of mailboxes with no storage limit. The default is n.
Maximum threshold for number of mailboxes	Specify the maximum number of mailboxes that can have no storage limit before an event is raised. The default is 300 mailboxes.
Exchange profile for NetIQ Corporationmc log on as account	Enter a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Enter a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of mailboxes with no storage limit exceeds the threshold. The default value is 5 (red event indicator).

MailboxStoreMountStatus

Use this Knowledge Script to monitor the mount status of one or more mailbox stores. When a mailbox store is unmounted, the Exchange Server cannot store information in it or read information from it.

Resource Object

Information Store folder, Mailbox Store object

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a mailbox store is unmounted. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns 100 if the mailbox store is mounted, 0 if the mailbox store is unmounted. The default option is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a mailbox store is unmounted. The default is 5 (red event indicator).

MsgAvgLocalDlvryTimeByIntrv

Use this Knowledge Script to monitor the average delivery time for local messages since the last time the script ran.

Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if average delivery time exceeds the threshold. The default is y.
Collect averages data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the average delivery time since the last time the script ran. The default is n.
Collect totals data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of messages and the total elapsed deliver time from which the average was derived. The default is n.
Maximum threshold for the average local delivery time.	Specify the highest average amount of time that it can take for local messages to be delivered before an event is raised. The default is 300 seconds.
Date format in message tracking log	Set this to be the same as the date format you are using in your message tracking log. The default is YYYY-MM-DD.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which average delivery time exceeds the threshold you set. The default is 5 (red event indicator).

MsgsAvgLocalDeliveryTime

Use this Knowledge Script to monitor the average delivery time for local messages for specified days. You can specify the interval to be a number of past days or start and stop dates.

Either interval specification looks at entries in the message tracking logs for the indicated days. If *Past N days to average messages* is 1, it looks at all the entries in today's log, since midnight, when it started, regardless of what time of day it is now. If *Past N days to average messages* is 2, it also examines the log from the day before that (all 24 hours of it).

Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete or disable the tracking logs.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if average delivery time exceeds the threshold you set. The default is y.
Collect averages data?	Set to **y** to collect data for charts and reports. If enabled data collection returns the average delivery time over the monitoring interval. The default is n.
Collect totals data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of messages and the total elapsed deliver time from which the average was derived. The default is n.
Maximum threshold for the average local delivery time.	Specify the maximum average delivery time that can have occurred since the last time this script was run. The default is 120 seconds.
Past N days to average messages	Specify the number of days over which to calculate the average delivery time. This value is ignored if you specify start and end dates. The default is 3 days.
Start date (YYYY/MM/DD)	Specify the start date for averaging delivery times.
End date (YYYY/MM/DD)	Specify the end date for averaging delivery times.
Date format in message tracking log	Set this to be the same as the date format you are using in your message tracking log. The default format is YYYY-MM-DD.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which local delivery time exceeds the threshold. The default is 5 (red event indicator).

MsgsBetweenAdminGroups

Use this Knowledge Script to monitor the total number and size of messages transferred between Exchange Admin Groups during the specified number of days or between specific start and end dates.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This Knowledge Script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days in local time may not represent the corresponding number of GMT hours. For example, if you monitor the previous day's messages (Count messages from past N days is set to 1), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Number of e-mail messages received from other Admin Groups. If this Knowledge Script cannot identify the Admin Group to which the sender belongs, the data detail message indicates the "Admin Group of <sender>". • Size of messages received in KB. • Number of e-mail messages sent to other Admin Groups. If this Knowledge Script cannot identify the Admin Group to which the recipient belongs, the data detail message indicates the "Admin Group of <recipient>". • Size of messages sent in KB. The default is n.
Maximum threshold for number of received mail messages	Specify the maximum number of messages that can be received from remote Admin Groups before an event is raised. The default is 300 messages.

Description	How to Set It
Maximum threshold for number of sent mail messages	Specify the maximum number of messages that can be sent from this Admin Group to other Admin Groups before an event is raised. The default value is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.
Count messages from past N days	Specify the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default value is 3 days. To set a specific start date and end date, leave this field blank. If you set a start and end date, this parameter is ignored.
Start date (YYYY/MM/DD)	Specify a start date for beginning the message count. If you do not specify a Start and End Date, the value for *Count messages from past N days* is used.
End date (YYYY/MM/DD)	Specify the end date for the message count. If you do not specify a Start and End Date, the value for *Count messages from past N days* is used.
Refresh server info at each interval?	Set to **y** to generate a table showing the Microsoft Exchange 2000 or Exchange Server 2003 servers and the admin groups to which they belong. In large organizations with hundred of servers, creating this table may take a while. Therefore, this parameter allows you to decide whether to create the table every time the script runs. If the customer environment is pretty static, there is little need to create the table. On the other hand, if the customer environment is very dynamic and the servers are moved across different admin groups quite often, then it is preferable to set this parameter to **y**. The default is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsBtwnAdmnGrpsByInterval

Use this Knowledge Script to monitor the number and size of messages sent to an Exchange Admin Group or received from an Exchange Admin Group during the monitoring interval.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns data collected during the monitoring interval: • Number of mail messages received from other Admin Groups. If this Knowledge Script cannot identify the Admin Group to which the sender belongs, the data detail message indicates the "Admin Group of <sender>". • Size of messages received in KB • Number of mail messages sent to other Admin Groups. If this Knowledge Script cannot identify the Admin Group to which the recipient belongs, the data detail message indicates the "Admin Group of <recipient>". • Size of messages sent in KB The default is n.
Maximum threshold for number of received mail messages	Specify the maximum number of messages that can be received from remote Admin Groups before an event is raised. The default is 300 messages.
Maximum threshold for number of sent mail messages	Specify the maximum number of messages that can be sent from this Admin Group to other Admin Groups before an event is raised. The default is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.

Description	How to Set It
Refresh server info at each interval?	Set to **y** to generate a table showing the Microsoft Exchange 2000 or Exchange Server 2003 servers and the admin groups to which they belong. In large organizations with hundred of servers, creating this table may take a while. Therefore, this parameter allows you to decide whether to create the table every time the script runs. If the customer environment is pretty static, there is little need to create the table. On the other hand, if the customer environment is very dynamic and the servers are moved across different admin groups quite often, then it is preferable to set this parameter to **y**. The default is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsByServer

Use this Knowledge Script to monitor the number and size of messages transferred between a target Exchange Server and all connected servers during a specified number of days or from a specific start date to a specific end date.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days (in local time) may not represent the corresponding number of GMT hours. For example, if you monitor the previous day's messages (Count messages from past N days is set to 1), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Size (KB) of messages sent • Number of messages sent • Size (KB) of messages received • Number of messages received The default is n.
Maximum threshold for number of received mail messages	Specify the maximum number of messages that can be received from remote server before an event is raised. The default is 300 messages.
Maximum threshold for number of sent mail messages	Specify the maximum number of messages that can be sent from this server to other servers before an event is raised. The default is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.

Description	How to Set It
Count messages from past N days	Enter the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default is 3 days. To set a specific start date and end date, leave this field blank. If you set a start and end date, this parameter is ignored.
Start date	Specify a start date for beginning the message count. Use the YYYY/MM/DD format.
End date	Specify a end date for the message count. Use the YYYY/MM/DD format.
Refresh server info at each interval (Exchange 2000 or Exchange 2003 only)?	Specify whether this script should dynamically create a table that describes which Exchange servers belong to which admin groups at each interval. In large organizations, creating this table can take a significant period of time. Therefore, decide whether to create the table every time the script runs based on the characteristics of your Exchange environment: • If your environment tends to remain static with few (if any) changes, you should not need to create the table and can set this parameter to **n**. • If your environment tends to be dynamic, with servers often moved from one admin group to another, you should set this parameter to **y**. The default is n.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsByServerByInterval

Use this Knowledge Script to monitor the number and size of messages transferred between a target Exchange Server and all connected servers during the monitoring interval.

In the parameters described below, the term "messages received" refers to the messages that the target Exchange Server received. "Messages sent" refers to the messages that the target Exchange Server sent to all connected Exchange Servers.

To use this script, you must enable the Tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange Server installation program sets up the share. If you install Exchange Server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns data collected during the monitoring interval: • Size (KB) of messages sent • Number of messages sent • Size (KB) of messages received • Number of messages received The default is n.
Maximum threshold for number of received mail messages	Specify the maximum number of messages the target Exchange server can receive before an event is raised. The default is 300 messages.
Maximum threshold for number of sent mail messages	Specify the maximum number of messages that can be sent from the target Exchange Server to connected Exchange Servers before an event is raised. The default is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.

Description	How to Set It
Refresh server info at each interval (Exchange 2000 only)?	Specify whether this script should dynamically create a table that describes which Exchange 2000 or Exchange Server 2003 servers belong to which admin groups at each interval. In large organizations, creating this table can take a significant period of time. Therefore, decide whether to create the table every time the script runs based on the characteristics of your Exchange 2000 or Exchange Server 2003 environment: • If your environment tends to remain static with few (if any) changes, you should not need to create the table and can set this parameter to **n**. • If your environment tends to be dynamic, with servers often moved from one admin group to another, you should set this parameter to **y**. The default is n.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsBySize

Use this Knowledge Script to monitor the number of messages transferred in different size ranges over a specified number of days or from a specific start date to a specific end date. This script checks the size of messages sent and received during a specified period and tracks the number of messages by size.

This script provides useful report data to help you monitor message traffic on a daily or weekly basis.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Microsoft Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This Knowledge Script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days (in local time) may not represent the corresponding number of GMT hours. For example, if you monitor the previous day's messages (Count messages from past N days is set to 1), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Range for message size (comma separated)	Specify the size ranges for tracking messages, specified in KB, separated by commas. For example, if you set the range to `10,50,100`, information is returned for the number of messages from 0-10 KB, 10-50 KB, 50-100 KB, and 100+ KB. The default range is 1,2,10,50,100,500.
Collect data for local messages (delivered)?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of locally delivered mail messages in each size category. The default is y.
Collect data for remote messages (received)?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of mail messages received from a non-local mailbox in each size category. The default is y.
Collect data for remote messages (sent)?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of mail messages sent to a non-local mailbox in each size category. The default is y.

Description	How to Set It
Count messages from past N days	Specify the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default value is 8 days. To set a specific start date and end date, leave this field blank. If you set a Start Date and End Date, this parameter is ignored.
Start date	Enter a start date for beginning the message count. Use the YYYY/MM/DD format.
End date	Enter an end date for the message count. Use the YYYY/MM/DD format.

MsgsOfSystem

Use this Knowledge Script to monitor the load of public folder replication messages between Microsoft Exchange sites and Microsoft Exchange 2000 or Exchange Server 2003 Admin Groups.

To replicate public folder information between sites or Admin Groups, Microsoft Exchange sends system messages. This script monitors the number and size of the Exchange system messages:

- Sent from the public information store to public information store on another Exchange site or Admin Group.
- Received by the public information store from the public information store on another Exchange site or Admin Group.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This Knowledge Script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days (in local time) may not represent the corresponding number of GMT hours.

For example, if you monitor the previous day's messages (*Count messages from past N days* is set to **1**), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number or size of any kind of system messages exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number and size of inbound and outbound messages for public folder and directory replication. The default is n.
Maximum threshold for number of system messages	Specify the maximum number of system messages that can be sent or received by the public information store before an event is raised. The default is 3000 messages.

Description	How to Set It
Maximum threshold for size of system messages	Specify the maximum size (in KB) for system messages sent or received by the public information store. An event is raised if messages exceed this size The default is 3000 KB.
Count messages from past N days	Specify the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default value is 3 days. To set a specific start date and end date, leave this field blank. If you set a Start Date and End Date, this parameter is ignored.
Start date	Specify a start date for beginning the message count. Use the MM/DD/YY format.
End date	Specify an end date for the message count. Use the MM/DD/YY format.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsOpenedByOWA

Use this Knowledge Script to monitor the number of messages opened by Outlook Web Access (OWA). This script raises an event if the number of opened messages exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of messages opened by OWA exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the difference between the number of messages opened by OWA during the current monitoring interval and the number of messages opened during the previous monitoring interval. The default is n.
Compare to previous monitoring interval?	Set to **y** to compare the number of messages opened by OWA during the current monitoring interval with the number of messages opened by OWA during the previous monitoring interval. The default is y. **Note** If set to n, data collection returns *only* the number of messages opened by OWA during the current monitoring interval.
Maximum threshold for the number of messages	Specify the maximum number of messages that OWA can open before an event is raised. The default is 99 messages.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number of opened messages exceeds the threshold. The default is 5 (red event indicator).

MsgsSentByOWA

Use this Knowledge Script to monitor the number of messages sent by Outlook Web Access (OWA). This script raises an event if the number of messages sent exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of messages sent by OWA exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the difference between the number of messages sent by OWA during the current monitoring interval and the number of messages sent during the previous monitoring interval. The default is n.
Compare to previous monitoring interval?	Set to **y** to compare the number of messages sent by OWA during the current monitoring interval with the number of messages sent by OWA during the previous monitoring interval. The default is y. **Note** If set to n, data collection returns *only* the number of messages sent by OWA during the current monitoring interval.
Maximum threshold for the number of messages	Specify the maximum number of messages that OWA can send before an event is raised. The default is 99 messages.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number of sent messages exceeds the threshold. The default is 5 (red event indicator).

MsgsSpecificDomain

Use this Knowledge Script to monitor the total number and size of messages transferred through an Internet Mail Connector (IMC) to and from a specific domain during a specified number of days or from a specific start date to a specific end date. In Exchange 2000 and Exchange Server 2003, the IMC has been replaced by the SMTP service.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This Knowledge Script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days (in local time) may not represent the corresponding number of GMT hours. For example, if you monitor the previous day's messages (Count messages from past N days is set to 1), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Number of messages received from the specified domain(s) • Size of messages received from the specified domain(s) in KB • Number of messages sent to the specified domain(s) • Size of messages sent to the specified domain(s) in KB The default is n.
Maximum threshold for number of received messages	Specify the maximum number of messages that can be received from the specified domain before an event is raised. The default is 300 messages.
Maximum threshold for number of sent messages	Specify the maximum number of messages that can be sent from this site to the specified domain before an event is raised. The default is 300 messages.

Description	How to Set It
List of domain names (comma separated)	Provide the name of the domain you want to monitor. You can enter multiple domain names separated by commas. For example: `microsoft.com,netiq.com`
Count messages from past N days	Specify the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default value is 3 days. If you set a start and end date, this parameter is ignored.
Start date	Specify a start date for beginning the message count. Use the YYYY/MM/DD format.
End date	Specify an end date for the message count. Use the YYYY/MM/DD format.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

Example of How This Script is Used

You can use this Knowledge Script to check the number and size of mail messages from a specific Internet domain. For example, to check the number of messages to and from NetIQ Corporation Corporation in the last 30 days, you would enter netiq.com for the Domain name parameter and 30 for the *Count messages from past N days* parameter.

MsgsSpecificDomainByInterval

Use this Knowledge Script to monitor the total number and size of messages transferred through an Internet Mail Connector (IMC) to and from a specific domain during the monitoring interval. In Microsoft Exchange 2000 and Exchange Server 2003, the IMC has been replaced by the SMTP service.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following data collected during the monitoring interval: • Size (KB) of messages sent to other domains • Number of messages sent to other domains • Size (KB) of messages received from other domains • Number of messages received from other domains The default is n.
Maximum threshold for number of received messages	Specify the maximum number of messages that can be received from remote domains before an event is raised. The default is 300 messages.
Maximum threshold for number of sent messages	Specify the maximum number of messages that can be sent to other domains before an event is raised. The default is 300 messages.
List of domain names (comma separated)	Provide the name of the domain you want to monitor. You can enter multiple domain names separated by commas. For example: `microsoft.com,netiq.com`
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default value is 5 (red event indicator).

MsgsThroughConnector

This Knowledge Script monitors the total number and size of messages sent and received by one or more specified connectors on an Exchange site or router group during a specified number of days or from a specific start date to a specific end date. For Microsoft Exchange 2000 or Exchange Server 2003, this script monitors connectors to external mail systems only.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, ensure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days (in local time) may not represent the corresponding number of GMT hours. For example, if you monitor the previous day's messages (Count messages from past N days is set to 1), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number or size of messages sent from or received by monitored connectors exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Size (KB) of messages received by connectors • Number of messages received by connectors • Size (KB) of messages sent by connectors • Number of messages sent by connectors The default is n.
Maximum threshold for number of received messages	Specify the maximum number of messages that can be received by monitored connectors before an event is raised. The default is 300 messages.
Maximum threshold for number of sent messages	Specify the maximum number of messages that can be sent to monitored connectors before an event is raised. The default is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.
Count messages from past N days	Specify the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default value is 3 days. To set a specific start date and end date, leave this field blank. If you set a Start Date and End Date, this parameter is ignored.
List of connectors (comma separated)	Provide a list of connector names, separated by commas. The connector name is not case-sensitive. If you leave the connector list blank, this script returns data for all connectors. You cannot enter a single letter to get data for all connectors starting with that letter. You must enter the exact name of the connector. It may be easier to leave this parameter blank and check the data detail for the connectors of interest.
Start date	Specify a start date for beginning the message count. Use the YYYY/MM/DD format.
End date	Specify an end date for beginning the message count. Use the YYYY/MM/DD format.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsThroughSMTPService

Use this Knowledge Script to monitor the size and number of messages through the SMTP Service for the specified days. You can specify the interval to be a number of past days or start and stop dates.

Either interval specification looks at entries in the message tracking logs for the indicated days. If *Past N days to average messages* is 1, it looks at all the entries in today's log, since midnight, when it started, regardless of what time of day it is now. If *Past N days to average messages* is 2 it also examines the log from the day before that (all 24 hours of it).

Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of SMTP messages sent and received. The default is n.
Maximum threshold for number of received mail messages	Specify the maximum number of SMTP messages that can be received before an event is raised. The default is 300.
Maximum threshold for number of sent mail messages	Specify the maximum number of SMTP messages that can be sent before an event is raised. The default is 300.
Include Exchange system messages?	Set to **y** to include Exchange system messages. The default option is n.
Past N days to average messages	Specify the number of days over which to monitor SMTP messages. This value is ignored if you specify start and end dates. The default value is 3 days.
Start date (YYYY/MM/DD)	Specify the start date for monitoring SMTP messages.
End date (YYYY/MM/DD)	Specify the end date for monitoring SMTP messages.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsThruSMTPSvcByInterval

Use this Knowledge Script to monitor the size and number of messages through the SMTP Service during the monitoring interval. The monitoring interval is since the last time the script ran.

Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of SMTP messages sent and received. The default is n.
Maximum threshold for number of received mail messages	Specify the maximum number of SMTP messages that can be received before an event is raised. The default is 300.
Maximum threshold for number of sent mail messages	Specify the maximum number of SMTP messages that can be sent before an event is raised. The default is 300.
Include Exchange system messages?	Set to **y** to include Exchange system messages. The default is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsWithinAdminGroup

Use this Knowledge Script to monitor the total number and size of messages transferred between Exchange servers in the same Admin Group during the specified number of days or from a specific start date to a specific end date.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days (in local time) may not represent the corresponding number of GMT hours. For example, if you monitor the previous day's messages (Count messages from past N days is set to 1), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when a threshold is exceeded. The default option is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of received and sent messages. The default is n.
Maximum threshold for number of received messages	Specify the maximum number of messages that can be received from other Exchange servers within the Admin Group before an event is raised. The default is 300 messages.
Maximum threshold for number of sent messages	Specify the maximum number of messages that can be sent from this Exchange server to other Exchange servers in the same Admin Group before an event is raised. The default is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default option is n.
Count messages from past N days	Specify the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default value is 3 days. If you set a start and end date, the number of previous days parameter is ignored.

Description	How to Set It
Start date (YYYY/MM/DD)	Specify a start date for beginning the message count.
End date (YYYY/MM/DD)	Specify an end date for stopping the message count.
Refresh server info at each interval?	Set to **y** to generate a table showing the Exchange 2000 or Exchange Server 2003 servers and the admin groups to which they belong. In large organizations with hundred of servers, creating this table may take a while. Therefore, this parameter allows you to decide whether to create the table every time the script runs. If the customer environment is pretty static, there is little need to create the table. On the other hand, if the customer environment is very dynamic and the servers are frequently moved across different admin groups, then it is preferable to set this parameter to **y**. The default is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsWthnAdmnGrpByInterval

Use this Knowledge Script to monitor the total number and size of messages sent and received between Exchange servers in the same Admin Group since last time the Knowledge Script ran (a delta value).

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following data collected during the monitoring interval: • Size (KB) of messages sent within this Admin Group • Number of messages sent within this Admin Group • Size (KB) of messages received within this Admin Group • Number of messages received within this Admin Group The default is n.
Maximum threshold for number of received messages	Specify the maximum number of messages that can be received by this server from other Exchange servers within this Admin Group before an event is raised. The default is 300 messages.
Maximum threshold for number of sent messages	Specify the maximum number of messages that can be sent from other Exchange servers within this Admin Group to this server before an event is raised. The default is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.
Refresh server info at each interval?	Set to **y** to generate a table showing the Exchange servers and the Admin Groups to which they belong. In large organizations with hundred of servers, creating this table may take a while. Therefore, this parameter allows you to decide whether to create the table every time the script runs. If your environment is pretty static, there is little need to create the table. On the other hand, if your environment is very dynamic and the servers are moved frequently across different Admin Groups, then it is preferable to set this parameter to **y**. The default is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number of received or sent messages exceeds the threshold. The default is 5 (red event indicator).

MTAConnectionQueueLength

Use this Knowledge Script to monitor the queue length of all message transfer agent (MTA) connections, including the MTAs to other servers in the site, public and private information stores, and any installed connectors (such as X.400 Connectors). If the server is a replication bridgehead, the MTA will also have a queue to the directory on its server.

You specify the maximum number of queued inbound and outbound messages, the maximum number of queued recipients, and the number of consecutive times the threshold can be exceeded before raising an event. This script raises an event if the number of queued inbound messages, queued outbound messages, or queued recipients exceeds the threshold you set.

Resource Object

Information Store folder

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the queue length for an MTA connection exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the queue length for each MTA connection. The default is n.
Maximum threshold for number of inbound messages	Specify the maximum number of inbound messages that can be queued before an event is raised. The default is 10000 messages.
Maximum threshold for number of outbound messages	Specify the maximum number of outbound messages that can be queued before an event is raised. The default is 10000 messages.
Maximum threshold for total number of messages	Specify the maximum total number of messages that can be queued before an event is raised The default is 100 messages.
Maximum threshold for number queued recipients	Specify the maximum number of recipients that can be queued before an event is raised. The default is 100 recipients.
List of MTA connection queues to monitor	Provide the names of the MTA connection queues to monitor (case-sensitive) in a comma-separated list or specify **ALL** to monitor all MTA connection queues. The default is ALL.

Description	How to Set It
Consecutive number of times before an event	Specify the consecutive number of intervals the threshold for queued messages or recipients can be exceeded before the Knowledge Script raises an event. The default is 5 consecutive intervals. Because queued messages or queued recipients can have periodic spikes, you may want to set this parameter to a higher value to filter out unnecessary events. For example, you may want to allow the number of queued messages to exceed the threshold 3 to 4 times before you are alerted.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

NNTPConnections

Use this Knowledge Script to monitor the total number of inbound and outbound connections to the Network News Transfer Protocol (NNTP) service. This script raises an event if the number of connections exceeds the threshold you set.

Resource Object

NNTP Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Total connections • Current connections • Total SSL connections • Total outbound connections The default is n.
Maximum threshold for total number of NNTP connections	Specify the maximum number of inbound and outbound NNTP connections that can have occurred since the server was last started. This script raises an event if the number of connections exceeds this threshold. The default is 500 connections.
Maximum threshold for number of outbound NNTP connections	Specify the maximum number of outbound NNTP connections that can have occurred since the NNTP server was last started. This script raises an event if the number of connections exceeds this threshold. The default is 1000 connections.
Maximum threshold for number of current NNTP connections	Specify the maximum number of concurrent NNTP connections that can occur before an event is raised. The default is 100 connections.
Maximum threshold for number of SSL connections	Specify the maximum number of SSL connections that can occur before an event is raised. The default is 1000 connections.
Consecutive number of times before an event	Specify the maximum number of consecutive times that each connection threshold can be exceeded before an event is raised. For example, if this parameter is set to 3 and the number of SSL connections exceeds the threshold each time the job runs, this script raises an event the third time the job runs. The default is 5 consecutive occurrences.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

NumberOfMailboxes

Use this Knowledge Script to monitor the total number of Exchange mailboxes. This script raises an event if the number of mailboxes exceeds the threshold you set.

On a computer with more than one virtual server, the total number of mailboxes is calculated as the total number of mailboxes for all virtual servers on the computer.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of mailboxes on the Exchange server exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of mailboxes found. The default is n.
Maximum threshold for number of mailboxes	Specify the maximum number of mailboxes that can be on an Exchange server before an event is raised. The default is 300 mailboxes.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mailbox alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of mailboxes exceeds the threshold. The default is 5 (red event indicator).

PFAclChanges

This Knowledge Script checks for changes in the access control lists for each folder in the public information store. This script raises an event if the script cannot collect information for a public folder.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of access control list changes exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of changes to a public folder's access control list. The default is n.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Maximum threshold for number of ACL changes	Specify the maximum number of changes to the public folder's access control list that can occur before an event is raised. The default is 0 (zero).
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default value is 5 (red event indicator).

PFAclInfo

This Knowledge Script collects data about the access control list for each folder in the public information store. This script raises an event if the script cannot collect data about a public information store.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data cannot be collected. The default is 5 (red event indicator).

PFInfo

This Knowledge Script monitors the number and size of public folders, and the number of messages in the public folders. You can set the data collection level to configure the level of collected public folder data. For more information, see "Setting the Level of Data Collection" on page 1889.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of public folders, the total size of all public folders, or the number of messages in all public folders exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following information, depending on the level of data detail you specify: • Number of public folders • Total size for all public folders (KB) • Number of messages stored in public folders For more information, see "Setting the Level of Data Collection" on page 1889. The default is n.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Maximum threshold for number of public folders	Specify the maximum number of public folders that can exist before an event is raised. The default is 100 public folders.

Description	How to Set It
Maximum threshold for size of file space (MB)	Specify the maximum size public folders can attain before an event is raised. The default is 300 MB.
Maximum threshold for number of messages	Specify the maximum number of messages that public folders can contain before an event is raised. The default is 30000 messages.
Character to separate data detail columns	Provide a character to use to separate the columns in the detail data. The default character is "|". If you change this parameter to Null, a Tab character is specified.
Detail level (1-3) for data collection	Specify a value (1, 2, or 3) to specify the level of data collection. The default value is 3. For more information, see "Setting the Level of Data Collection" on page 1889.
Range of message size	Monitor the number of messages in a range of sizes by specifying each size range in a comma-separated list. Specify the message size in kilobytes (KB). For example, if you enter "100,500,1000", this script returns the number of messages that are: • Less than 100 KB • Between 100 KB and 500 KB • Between 500 KB and 1000 KB • Greater than 1000 KB The default is "100,500,1000,2000".
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

Setting the Level of Data Collection

If you set the *Detail level (1-3) for data collection* parameter to **1**, the script returns the following information:

- Name of the public folder
- Size of messages in the public folder
- Number of messages in the public folder
- Path of the public folder
- Creation time of the public folder
- Last modification time of the public folder
- Last access time of the public folder
- Number of attachments in the public folder
- Number of messages in the public folder which have attachments
- Number of owners of the public folder

If you set the *Detail level (1-3) for data collection* parameter to **2**, the script returns the all of the information in level 1, plus the following additional information:

- Oldest message creation time
- Oldest message modification time
- Newest message creation time
- Newest message modification time

If you set the **Detail level (1-3) for data collection** to **3**, the script returns the all of the information in levels 1 and 2, plus the number of messages in user-defined size ranges. For example, the number of messages that are between one and ten KB.

PFReplicationByObj

This Knowledge Script monitors public folder replication between Exchange servers by updating a test object on a local public folder and checking the replica folder on one or more remote Exchange servers for the replicated object.

Before you run this script:

- Create a public folder on the local Exchange server for creating and updating the test object.
- Configure this public folder to be hosted by the remote Exchange servers you want to test.

Note

This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of unreplicated test objects on a remote Exchange server exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the replication status of the test object on each remote Exchange server. The default is n.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It

List of remote servers to host test object	Specify a list of remote Exchange servers that host a replica of the test object on the local Exchange server. Use the following syntax:
	`<computer>(/O=<organization>/OU=<administrative group>`
	Where:
	• ***computer*** specifies the name of the computer on which the Exchange server is installed
	• ***organization*** specifies the name of the Exchange organization to which the server belongs
	• ***administrative group*** specifies the name of the Exchange administrative group to which the server belongs
	Separate more than one server name using "|", for example:
	`Server1(/O=Org1/OU=AdminGrp1)|Server2(/O=Org2/OU=AdminGrp2)`

Local public folder to maintain test object	Specify the name of the local public folder that the Knowledge Script uses to create and update the test object. The folder name must start with "\". For example, to specify a public folder named "aaa", enter "\aaa". The default is "\".
Maximum threshold for number of unreplicated changes	Specify the maximum number of unreplicated changes that can occur between the local public folder and a public folder on a remote Exchange server. This script raises an event if the number of unreplicated changes exceeds the threshold. The default is 5 unreplicated changes.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of unreplicated changes exceeds the threshold. The default is 5 (red event indicator).

POP3Accesses

Use this Knowledge Script to monitor the number of POP3 access operations. The POP3 access operations include `LAST`, `STAT`, `LIST`, `DEL`, `NOOP`, and `RSET` operations. This script raises an event if the total number of POP3 access operations exceeds the threshold you set.

Resource Object

POP3 Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of POP3 access operations exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled data collection returns the number of POP3 access operations. The default is n.
Maximum threshold for number of POP3 access operations	Specify the maximum number of POP3 access operations that can occur before an event is raised. The default is 10000 access operations.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

POP3Authenticate

Use this Knowledge Script to monitor the authentication of POP3 protocols. This script raises an event if the rate of failure of total authentications exceeds the threshold.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003, Protocols folder

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of authentication failures exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Number of authenticate commands received since startup • Number of authenticate commands per second • Number of authenticate command failures since startup The default is n.
Maximum threshold for number of authentication failures	Specify the maximum number of authentication failures that can have occurred since startup. This script raises an event if the number of failures exceeds this threshold. The default is 1000.
Consecutive number of times before an event	Specify the maximum number of consecutive times the threshold can be exceeded before this script raises an event. The default is 5 consecutive occurrences.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

POP3Connections

Use this Knowledge Script to monitor the number of current and total connections to the POP3 service. You specify the maximum number of current and total connections and the number of consecutive times the threshold can be exceeded before raising an event. This script raises an event if the current or the total connections exceed the threshold for the specified consecutive number of intervals.

Resource Object

POP3 Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Total connections • Current connections The default is n.
Maximum threshold for total number of connections	Specify the maximum number of POP3 connections that can have occurred since the POP3 server was last started. This script raises an event if the number of connections exceeds this threshold. The default is 1000 connections.
Maximum threshold for number of current POP3 connections	Specify the maximum number of POP3 connections that can occur during the current monitoring interval. This script raises an event if the number of connections exceeds the threshold. The default is 100 connections.
Consecutive number of times before an event	Specify the consecutive number of intervals the threshold for connections can be exceeded before raising an event. The default is 5 consecutive intervals. Because connections can have periodic spikes, you can set this parameter to a higher value to filter out unnecessary events. For example, you can allow the number of current connections to exceed the threshold 3 to 4 times before an event is raised.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ProtocolVSStatus

Use this Knowledge Script to monitor the status of HTTP, NNTP, POP3, IMAP4, and SMTP virtual servers. This script attempts to restart a virtual server that is detected as down.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Automatically restart service?	Set to **y** to automatically restart a service that is down. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns 100 if a monitored virtual server is up, 0 if a monitored virtual server is down. The default is n.
Event?	Set to **y** to raise an event if a service is down and restart fails or succeeds, or you do not want to restart. The default is y.
Severity: Failed to restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager fails to restart the service. The default is 5 (red event indicator).
Severity: Successful restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager successfully restarts the service. The default is 25 (blue event indicator).
Severity: Do not restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and you do not want AppManager to restart the service. The default value is 18 (yellow event indicator).

PublicStoreMountStatus

Use this Knowledge Script to monitor the mount status of one or more public stores. When a public store is unmounted, the Exchange Server cannot store information in it or read information from it.

Resource Object

Information Store folder, Public Store object

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a public store is unmounted. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns 100 if the public store is mounted, 0 if the public folder store is unmounted. The default is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a public store is unmounted. The default is 5 (red event indicator).

QueueStatus

Use this Knowledge Script to monitor the inbound and outbound message queue status of all X.400 and SMTP virtual servers, including the number, size, and elapsed time for messages that reside in a message queue. This script raises an event if the number, size, or elapsed time exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Once a day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Specify a protocol (X400, SMTP, or ALL)	Select one of the following to specify the protocols to monitor (not case-sensitive): • **X400** monitors the X.400 protocol. • **SMTP** monitors the SMTP protocol. • **ALL** monitors both X.400 and SMTP protocols. The default is ALL.
Collect total number of messages, queue sizes and elapsed time of queues?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of messages, queue size, and elapsed time of inbound and outbound message queues. The default is n.
Collect data for number of messages in queues?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of messages in a message queue. The default is n.
Threshold - Maximum for number of messages in queues	Specify the maximum number of messages that can be in a queue before an event is raised. The default is 1000.
Event for number of messages in queues?	Set to **y** to raise an event when the number of messages in queue exceeds the threshold. The default is y.
Event severity: Number of messages in queues	Set the event severity level, from 1 to 40, to specify the importance of an event in which the number of messages in queue exceeds the threshold. The default is 5.
Collect data for size of queues?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the size of a message queue. The default is n.
Threshold - Maximum for size of queues	Specify the maximum size a queue can attain before an event is raised. The default is 100 MB.
Event for size of queues?	Set to **y** to raise an event when the size of a message queue exceeds the threshold. The default is y.
Event severity: Size of queues	Set the event severity level, from 1 to 40, to specify the importance of an event in which the size of a message queue exceeds the threshold. The default is 5.
Collect data for elapsed time in queues?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the oldest messages in a message queue. The default is n.

Description	How to Set It
Threshold - Maximum for elapsed time in queues	Specify the maximum number of seconds a message can remain in queue before an event is raised. The default is 1000.
Event for elapsed time in queues?	Set to **y** to raise an event when a message spends too long in a queue. The default is y.
Event severity: Elapsed time in queues	Set the event severity level, from 1 to 40, to specify the importance of an event in which a message spends too long in a queue. The default is 5.

Report_Connectivity

Use this Knowledge Script to generate a report about the connectivity between Exchange 2000 Server and Exchange Server 2003. This report uses data collected by the Connectivity Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse [...]** to select the computers for your report.
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Data settings	
Hours or percentage on chart	Select whether to illustrate availability by **Hours** or by **Percentage**.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set the report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ISPrivateResourceSummary

Use this Knowledge Script to generate a report about the file space used by private information store folders and mailboxes. This report allows you to make a statistical analysis of the data point values over the time range you define for the report. This report uses data collected by the TopNISMailboxRes Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse [...]** to select the computers for your report.
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set the report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ISPublicResourceSummary

Use this Knowledge Script to generate a report about the file space used by public information store folders. This report allows you to make a statistical analysis of the data point values over the time range you define for the report. This report uses data collected by the TopNISPublicRes Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse [...]** to select the computers for your report.
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set the report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ServerLoad

Use this Knowledge Script to generate a report about the rate at which the Exchange server sends and receives messages and the rate at which the Exchange server processes the RPC packets. This report lets you aggregate the data by time period (minute, hour, or day) and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the ServerLoad Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse [...]** to select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (For example, each page shows the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval (for example, the average value for 1 Hour) • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ServerMessage

Use this Knowledge Script to generate a report about the total number of mail recipients, messages delivered, messages sent, messages submitted, the mailbox store, and the public information store. This report lets you aggregate the data by time period (minute, hour, or day) and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the ServerTotalMsg Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse [...]** to select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (For example, each page shows the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval (for example, the average value for 1 Hour) • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set report parameters as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ServerUsers

Use this Knowledge Script to generate a report about the number of users connected to the information store. This report lets you aggregate the data by time period (minute, hour, or day) and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the ServerUsers Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse [...]** to select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (For example, each page shows the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval (for example, the average value for 1 Hour) • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set report parameters as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopNMailboxesInfo

Use this Knowledge Script to generate a report about the file space (in MB) used by the top private information store folders or mailboxes.

This report uses data collected by the TopNISMailboxRes Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse [...]** to select the computers for your report.
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopNReceivers

Use this Knowledge Script to generate a report about which users received the most mail messages, and the total file size of messages received by the top users or by all users.

This report uses data collected by the TopNReceivers Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse [...]** to select the computers for your report.
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopNSenders

Use this Knowledge Script to generate a report about which users sent the most mail messages, and the total file size of messages sent by the top users or by all users.

This report uses data collected by the TopNSenders Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse [...]** to select the computers for your report.
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Select properties	Click **Browse [...]** to set the properties parameters as desired.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

ResponseTime

Use this Knowledge Script to check the mail response time between two or more Exchange 2000 servers or Exchange Server 2003 servers. This script cannot monitor more than one Exchange 2000 or Exchange Server 2003 virtual server.

If you only have one Exchange server, do not use this script. If you only have one Exchange server, this script incorrectly reports that the Exchange Server is down. To monitor response time for a single Exchange server, use the AppManager ResponseTime for Microsoft Exchange module.

This script determines if e-mail is delivered and the time it takes for the message to be delivered. In addition, this script raises an event if a reply to the test message is not received within the response time threshold you set.

To run this script on a group of Exchange servers, each server must have the same profile name.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

Note

This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 15 minutes**, which is appropriate if you are monitoring Exchange servers in a connected network.

If your Exchange servers rely on a remote WAN or LAN service (such as RAS) or a dial-up modem that is not always connected, you can set up server group folders to separate Exchange servers into different groups. Then you can set the schedule interval for this script to run on each folder based on each group's connection schedule.

For example, you can create one server group for your always-connected servers and a separate folder for offhours RAS connections and create two different sets of jobs with different schedules (frequently for your connected network and once a day or based on the scheduled connection time for the remote access servers). For information about setting up server groups, see the *User Guide for AppManager*.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the response time threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the response time in seconds for each Exchange server. The default is y.
Exchange profile for NetIQmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager. This is especially true if you are running this script on the top-level Exchange folder or Exchange server groups.
Mailbox alias for NetIQmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager. This is especially true if you are running this script on the top-level Exchange folder or Exchange server groups.
Maximum threshold for response (in seconds)	Specify the maximum number of seconds that can elapse from the time the test message is sent out until a reply should be received. The default response time is 120 seconds.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event which the response time threshold is exceeded. The default value is 5 (red event indicator).

Example of How This Script is Used

To measure response time, this Knowledge Script sends a test mail message to each of Exchange servers being tested, using the profile and mailbox alias name set up for the computer running the job using AppManager Security Manager or the parameters specified in this script. After the test message is delivered by the "sending" server, each of the "receiving" servers responds with a reply. The response time is the time it takes for the "sending" server to receive this reply from the mail recipient.

For example, assume you run this script on a server group folder with the Exchange servers Paris, Cabernet, Dynamo, Boston, and Nero. The **netiq-Paris** Exchange client on Paris sends a message to Cabernet, Dynamo, Boston, and Nero. If Cabernet **(netiq-Cabernet)** responds and Paris receives the reply 60 seconds later, the response time from Paris to Cabernet is 60 seconds.

Simultaneously, the **netiq-Cabernet** Exchange client on Cabernet is sending test messages to Paris, Dynamo, Boston, and Nero. If the reply from Paris **(netiq-Paris)** is received 90 seconds after delivery, then the response time from Cabernet to Paris is 90 seconds.

Although this example focuses on the communication and response time between Paris and Cabernet, the same send-and-reply operations are taking place for all of the servers in the group.

Locale Considerations

This Knowledge Script asks Exchange to send a delivery-receipt message when the test e-mail is delivered to the recipient. In the English version of AppManager, this script looks for a delivery-receipt e-mail whose subject line is "Delivered."

If the recipient uses an Exchange server configured with a different locale, the subject line of the response is the word "Delivered" translated into that locale's language.

The English version of AppManager does not recognize a non-English response and, likewise, the Japanese version of AppManager does not recognize a non-Japanese response.

ServerHealth

Use this Knowledge Script to monitor the health of the Exchange server. This script monitors the percentage of time that all processors on the Exchange server are busy and the percentage of elapsed time that the Exchange server process threads are used to execute instructions. In addition, this script raises an event if a monitored value exceeds the threshold you set.

This script tracks the following performance objects:

Object	Counter	Instance
Processor	% Processor Time	_Total
Process	% Processor Time	inetinfo
Process	% Processor Time	EMSMTA
Process	% Processor Time	STORE
Process	% Processor Time	MAD
Memory	Pages/sec	

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns either the current value or the delta value for each monitored performance counter. The default is n.
Compare to previous monitoring interval?	Set to **y** to compare the data collected in the current monitoring interval to the previous monitoring interval. If set to y, any graphs you create plot the comparison value rather than the total value. If set to y, the data collected and the thresholds you set can be positive or negative. The default is n.
Maximum threshold for total processor usage	Specify the maximum percentage of time that all the processors on the system can be busy executing non-idle threads. This value can be viewed as the fraction of the time spent doing useful work. On a multi-processor system, if all processors are always busy this is 100%, if all processors are 50% busy this is 50% and if 25%of the processors are 100% busy, this is 25%. The default is 99%.
Maximum threshold for processor usage by Exchange services	Specify the maximum percentage of elapsed processor time that all of the threads the Exchange server processes can use to execute instructions. Code executed to handle certain hardware interrupts or trap conditions may be counted. The default is 10%.

Description	How to Set It
Maximum threshold for total memory pages per second	Specify the maximum number of pages that can be read from the disk or written to the disk to resolve memory references. This value is the sum of pages input/sec and pages output/sec and includes paging traffic on behalf of the system Cache to access file data for applications and pages to and from non-cached, mapped memory files. The default is 200 memory pages per second. **Tip** This is the primary counter to observe if you are concerned about excessive memory pressure (thrashing), and the excessive paging that may result.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ServerHistory

Use this Knowledge Script to monitor the complete message history for an Exchange server. This script monitors the combined message count for the mailbox stores and public information stores.

This script raises an event if the number of messages exceeds the threshold you set.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following data: • Number of recipients that have received a message (message recipients delivered - private information or mailbox store). • Number of messages delivered (messages delivered - private information or mailbox store). • Number of messages sent (messages sent - private information or mailbox store). • Number of messages submitted (messages submitted - public information store). • Number of recipients that have received messages (message recipients delivered - public information store). • Number of messages sent (messages sent - public information store). • Number of Exchange users • MTA work queue length. The default is n.

Description	How to Set It
Maximum threshold for number of messages	Specify the total number of messages that can have occurred since startup before an event is raised. The default is 10000 messages. To track messages, this script monitors the following: Mailbox information store: • Total number of recipients that have received a message since startup (message recipients delivered). • Total number of messages delivered to all recipients since startup (messages delivered). • Total number of messages sent to other storage providers via Message Transfer Agent (MTA) since startup (messages sent). • Total number of messages submitted by clients since startup (messages submitted). Public information store: • Total number of recipients that have received a message since startup (message recipients delivered). • Total number of messages sent to other storage providers via MTA since startup (messages sent).
Maximum threshold for number of users	Specify the maximum number of users that can be connected to the private and public information store or mailbox store and public information store before an event is raised. The default is 500 users.
Maximum threshold for number of messages in work queue	Specify the maximum number of outstanding messages that can be in the work queue before an event is raised. Messages in the work queue have not yet been processed to completion by the MTA. The default is 5 messages.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ServerLoad

Use this Knowledge Script to monitor the load on the Exchange server. This script tracks the rate at which the Exchange server receives and submits messages per minute. This script also monitors the rate at which the Exchange server processes the RPC packets. This script raises an event if a threshold is exceeded.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following load information: • Rate of messages delivered per minute • Rate of messages submitted per minute • Rate of delivery for RPC packets per second **Note** The specific data streams you see will depend on the version of Exchange you are monitoring. The default is n.
Threshold for delivered private messages per minute	Specify the maximum rate at which recipients can receive private messages before an event is raised. The default is 500 per minute.
Threshold for submitted private messages per minute	Specify the maximum rate at which private messages can be submitted by clients before an event is raised. The default is 500 per minute.
Threshold for delivered public messages per minute	Specify the maximum rate at which recipients can receive public messages before an event is raised. The default is 500 per minute.
Threshold for submitted public messages per minute	Specify the maximum rate at which public messages can be submitted by clients before an event is raised. The default is 500 per minute.
Threshold for adjacent MTA associations	Specify the maximum number of open associations that this MTA can have to other MTAs before an event raised. The default is 100.
Threshold for processed RPC packets per second	Specify the maximum rate at which RPC packets can be processed before an event is raised. The default is 500 per second.
Threshold for address book browse operations per second	Specify the maximum rate at which address book clients can perform browse operation before an event is raised. The default is 150 per second.
Threshold for address book read operations per second	Specify the maximum rate at which address book clients can perform read operations before an event is raised. The default is 100 per second.

Description	How to Set It
Threshold for extended directory service read operations per second	Specify the maximum rate at which extended directory service clients can perform read operations before an event is raised. The default is 50 per second.
Threshold for directory service replication updates per second	Specify the maximum rate at which replication updates can be applied by the local directory service before an event is raised. The replication rate indicates how much replication activity is occurring on the server. The default is 50 per second.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ServerQueues

Use this Knowledge Script to monitor Exchange server queues, including the MTA work queue and the IS Private and IS Public send and receive queues. This script raises an event if a queue exceeds the threshold you set.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the queue length for each queue monitored. The default is n.
Threshold for number of messages in MTA work queue	Specify the maximum number of outstanding messages that can be in the work queue before an event is raised. The work queue contains messages not yet processed to completion by the MTA. The default is 20 messages.
Threshold for number of private messages in send queue	Specify the maximum number of private messages that can be in the send queue before an event is raised. The default is 20 messages.
Threshold for number of public messages in send queue	Specify the maximum number of public messages that can be in the send queue before an event is raised. The default is 20 messages.
Threshold for number of private messages in receive queue	Specify the maximum number of private messages that can be in the receive queue before an event is raised. The default is 20 messages.
Threshold for number of public messages in receive queue	Specify the maximum number of public messages that can be in the receive queue before an event is raised. The default is 20 messages.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ServerTotalMsg

Use this Knowledge Script to monitor the total number of messages for an Exchange server. You can set separate thresholds for the total number of mail recipients, the number of messages delivered, the number of messages sent, the number of messages submitted, and the number of messages waiting to be delivered for the mailbox store and public information store. This script raises an event if the server exceeds a threshold.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following information: • Number of recipients to whom messages were delivered • Number of messages delivered • Number of messages sent • Number of messages submitted • Number of messages still outstanding The default is n.
Maximum threshold for private message recipients	Specify the maximum number of recipients that can receive private messages before an event is raised. The default is 800.
Maximum threshold for private delivered messages	Specify the maximum number of private messages that can be delivered to all recipients before an event is raised. The default is 800. This parameter is applicable for the mailbox store on Exchange 2000 Server.
Maximum threshold for private sent messages	Specify the maximum number of private messages that can be sent to other storage providers by Message Transfer Agent (MTA). This script raises an event if the number of messages exceeds the threshold. The default is 800. This parameter is applicable for the mailbox store on Exchange 2000 Server.
Maximum threshold for private submitted messages	Specify the maximum number of private messages that can be submitted by clients before an event is raised. The default is 800. This parameter is applicable for the mailbox store on Exchange 2000 Server.

Description	How to Set It
Maximum threshold for private outstanding messages	Specify the maximum number of private messages that can be waiting for delivery before an event is raised. The default is 800. This parameter is applicable for the mailbox store on Exchange 2000 Server.
Maximum threshold for public message recipients	Specify the maximum number of recipients that can receive public messages before an event is raised. The default is 800.
Maximum threshold for public sent messages	Specify the maximum number of public messages that can be sent to other storage providers by Message Transfer Agent (MTA). This script raises an event if the number of messages exceeds the threshold. The default is 800.
Maximum threshold for public submitted messages	Specify the maximum number of public messages that can be submitted before an event is raised. The default is 800.
Maximum threshold for public outstanding messages	Specify the maximum number of public messages that can be waiting for delivery before an event is raised. The default is 800.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ServerUsers

Use this Knowledge Script to monitor the number of users connected to the information store. This script raises an event if the number of users exceeds the threshold you set.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of user connections exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of user connections. The default is n.
Maximum threshold for number of connected users	Specify the maximum number of users that can be connected to the information store before an event is raised. The default is 500 users.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of user connections exceeds the threshold. The default is 5 (red event indicator).

ServicesDown

Use this Knowledge Script to monitor the up and down status of Exchange services. This script checks services using the known order of dependency, which is managed by the Windows service controller. If any service is detected as down, this script can automatically attempt to restart the service and any dependent services.

Note
In Exchange Server 2003, the Exchange Event Service stops automatically if it does not have any work to do. If you are using the ServicesDown Knowledge Script to monitor this service, you get an event every time this service shuts down. If this script is set to restart it, you may get an event every time the script runs if the service continues to stop itself.

Resource Object

Exchange 2000 Server or Exchange Server 2003, Exchange Services folder.

Default Schedule

The default interval is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Automatically re-start service?	Set to **y** to automatically restart down services. The default is y.
Severity: Failed to restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager could not restart the service. The default is 5 (red event indicator).
Severity: Successful restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager restarted the service. The default is 25 (blue event indicator).
Severity: Do not restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and you do not want to restart the service. The default is 18 (yellow event indicator).
Check MSExchangeCCMC?	Set to **y** to check the Exchange Connector for Lotus cc:Mail. The default is n.
Check MSExchangeChat?	Set to **y** to check the Microsoft Exchange Chat service. The default is n.
Check MSExchangeCOCO?	Set to **y** to check the Exchange Connectivity Controller. The default is n.
Check MSExchangeDX?	Set to **y** to check the Exchange Directory Synchronization service. The default is y.
Check MSExchangeES?	Set to **y** to check the Exchange Event Service. The default is n.
Check MSExchangeFB?	Set to **y** to check the Exchange Schedule and Free/Busy Connector service. The default is n.
Check MSExchangeGWRtr?	Set to **y** to check the Microsoft Exchange Router for Novell GroupWise. The default is n.
Check MSExchangeIS?	Set to **y** to check the Exchange Information Store service. The default is y.

Description	How to Set It
Check MSExchangeKMS?	Set to y to check the Exchange Key Management Server service. The default is n.
Check MSExchangeMSMI?	Set to **y** to check the MS Mail Connector Interchange service. The default is n.
Check MSExchangeMTA?	Set to **y** to check the Exchange Message Transfer Agent service. The default is y.
Check MSExchangePCMTA?	Set to **y** to check the MS Mail Connector (PC) MTA service. The default is n.
Check MSExchangeSA?	Set to **y** to check the Exchange System Attendant. The default is y.
Check MSExchangeWEB?	Set to **y** to check the Exchange Web Component. The default is y.
Check MSExchangeDS?	Set to **y** to check the Exchange Directory service. The default is y.
Check MSExchangeIMC?	Set to **y** to check the Exchange Internet Mail Connector service. The default is n.
Check MSExchangeSRS?	Set to **y** to check the Site Replication Service. The default is y.
List of services (comma separated)	Specify any additional services you want to monitor. Separate the names by commas with no spaces.

SMTPConnectivity

Use this Knowledge Script to verify connectivity between an Exchange Server and one or more Internet domains through an SMTP gateway. The script verifies connectivity by sending a message to a non-existent user account and examining the resulting non-delivery report (NDR).

Note

Receiving no report is interpreted as a connectivity failure. If you do not allow NDRs, for example, for security reasons, try using the SMTPConnectivityExKnowledge Script, which allows you to send a message to an existing account and examine a delivery report (DR).

If you are checking the domain `netiq.com`, this script sends a test message to `a++++@netiq.com`. This is presumed to be a non-existent account. When the message cannot be delivered to the recipient, the Internet Mail Service sends an NDR to the Exchange mailbox associated with the AppManager agent to indicate the failure. This script scans the subject and body of the NDR for strings that indicate the status of the SMTP gateway host:

- If the test message is delivered to the SMTP host, the NDR says that the user does not exist, but indicates that there is connectivity between Exchange and the SMTP gateway.
- If the test message generates an NDR because it fails to reach the SMTP host, indicates that there is no connectivity between Exchange and the SMTP gateway.

Therefore, to configure this script, you need to know the strings that appear in an NDR subject and body when the domain you are checking is available or unavailable.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

To use this Knowledge Script effectively, perform the following before running this script:

1. Verify that your Exchange Server uses the Internet Mail Connector or Internet Mail Service to connect to the Internet through an SMTP gateway.
2. Verify how long it takes the gateway to forward NDRs to the mailbox associated with the AppManager agent service account. If the AppManager agent mailbox does not receive NDRs before the next time it runs, it is considered a connectivity failure.
3. As a test, send an e-mail message to an invalid user account on a valid domain, for example, `a++++@netiq.com`, and see how long it takes for the NDR to come back. If the NDR does not come back before this Knowledge Script runs again, it is interpreted as a domain connectivity failure.
4. If the AppManager agent mailbox successfully receives the NDR, check the subject line and message body for the text strings that indicate the status of the SMTP server. The subject and body text in an NDR can vary for each domain, but typically you can determine the status of the host by checking for the following information:
   - Check the subject line for the keyword string indicating that the test message was not delivered. For example, `Undeliverable` indicates that either the host is unavailable, or the user does not exist, but you cannot tell which until you check the body.
   - Check the body of the message for the same indications. A text string such as `Destination server for this recipient could not be found` indicates no connectivity. A string such as `e-mail account does not exist` means that there is connectivity, even though there is no such account.

   If the subject and the body of the NDR do not help you to determine text strings to use for checking the availability of the SMTP host, try sending a test message to another domain.

5. Repeat this test message when the host is down.

Note

This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event for connectivity status. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns a value of 100 if the connection between the Exchange Server and Internet domain is up or a value of 0 if the connection is down during the interval. The detail message includes the name of each Exchange Server and domain connection checked. When there is connectivity, this script also collects the response time in seconds. The default is y.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange Server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange Server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
List of domains	Specify the domain names that you want to check. If specifying more than one, the Subject and Body Keywords are matched to all of them. Use a pipe character (|) to separate multiple strings. For example: `netiq.com|abc.com` The default domain is netiq.com.

Description	How to Set It
Subject keywords when ...	Provide a keyword string found in the subject line of the NDR message that indicates whether the host status is up or down. • **... host is up**. Enter a keyword string that appears in the subject line of the NDR when mail delivery fails but the host is available. The default is `Undeliverable`. • **... host is down**. Enter a keyword string that appears in the subject line of the NDR when mail delivery fails because the host is not available. The default is `Undeliverable`. If specifying a string for more than one Internet domain, the order in which you specify the keyword strings must correspond to the list of Internet domains. Use a pipe character (|) to separate multiple strings. **Note** Depending on your environment, you may need to set keyword strings for both the subject line and the message body to determine the availability of the host server. For more information, see "Understanding How Keyword Strings Work" on page 1938. If you do not specify a value for a parameter, the parameter always matches. If you do not want to use a particular parameter to determine connectivity, you can enter a "garbage" string that does not appear in the NDR.
Body keywords when ...	Provide a keyword string found in the body of the NDR message that indicates whether the host status is up or down. • **... host is up**. Enter a keyword string that appears in the message body of the NDR when mail delivery fails but the host is available. The default is `e-mail account does not exist`. • **... host is down**. Enter a keyword string that appears in the message body of the NDR when mail delivery fails because the host is not available. The default is `destination server for this recipient could not be found`. If specifying a string for more than one Internet domain, the order in which you specify the keyword strings must correspond to the list of Internet domains. Use a pipe character (|) to separate multiple strings. **Note** Depending on your environment, you may need to set keyword strings for both the subject line and the message body to determine the availability of the host server. For more information, see "Understanding How Keyword Strings Work" on page 1938. If you do not specify a value for a parameter, the parameter always matches. If you do not want to use a particular parameter to determine connectivity, you can enter a "garbage" string that does not appear in the NDR.
Maximum threshold for a response	Specify the maximum number of seconds in which you expect to get a response. If a response takes longer than this number of seconds, this script raises an event. The default is 120 seconds.
Description file on managed client	Set to **y** to use the keyword strings specified in a file on the managed client to describe the host status. If this parameter is set to y, the subject and body keywords are ignored. The default is n. For more information, see "Understanding How Description Files Work" on page 1939.

Description	How to Set It

Description file name	Provide the full path to the file on the agent computer that contains the description file. For example:
	`C:\temp\msgsample.txt`
	To use the specified description file, you must set the Description file on managed client parameter to y.
	The default is `C:\temp\aa.txt`.
	You can use the UNC format to specify the path. For example:
	`\\ENG\appdev\mylog.txt`
	Tip You can only specify one file name for any job instance. To monitor multiple files, create separate Knowledge Script jobs.

Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event. The default is 5 (red event indicator).

Understanding How Keyword Strings Work

AppManager compares the text in the subject and message body of the NDR to the Subject and Body keyword strings you specify. As the script runs, it searches the subject and body of the NDR from left to right for a string that matches the string you have specified, including any spaces. The search is not case-sensitive, however, so you can specify the keyword strings in upper, lower, or mixed case.

For NDRs that substitute the SMTP address or host name in the message body, you can simplify the keyword string by using the following:

- `%%` substitutes the SMTP address. For example, if the body of an NDR contains `User a++++@netiq.com does not exist`, you can search for this string by specifying `User %% does not exist`.
- `##` substitutes the host name. For example, if the body of an NDR contains `Host abc.com does not exist`, you can search for this string by specifying `Host ## does not exist`.

If you specify keyword strings for multiple parameters, AppManager uses rules of precedence to determine the status of the host computer. If the script finds a match to the keyword string you specify for either Subject keywords when host is down, Body keywords when host is down, or both, the script reports the host as unavailable, even if there is also a match for the Subject keywords when host is up, Body keywords when host is up, or both. In general, the only time the script reports the host available is if:

- The report subject line contains no matches to the "Subject keywords when host is down" keyword string, and...
- The report body contains no matches to the "Body keywords when host is down" keyword string, and...
- The report contains matches for both the "Subject keywords when host is up" keyword string and "Body keywords when host is up" keyword string.

If you do not specify a text string for a parameter, the parameter is always considered a match. To configure a parameter to never match, enter a "garbage" text string that does not appear anywhere in the NDR.

Using Keyword Strings to Determine Availability

To configure this Knowledge Script, you must provide specific strings that indicate whether a domain host is available for mail delivery. To do this, you must be familiar with the content of delivery reports (DRs) and NDRs and how to select an appropriate string for which to search.

You can configure this script to identify the host status using the following keyword strings:

Parameter	What to Specify
Subject keywords when host is up	Undeliverable
Subject keywords when host is down	Mail System Error - Returned Mail
Body keywords when host is up	The recipient name is not recognized
Body keywords when host is down	Host netiq.com not found

Understanding How Description Files Work

You can configure this Knowledge Script to use keyword strings specified in the Values tab of the Knowledge Script Properties dialog box or a *description file* on the agent computer.

A description file resides on the agent computer and specifies the keyword strings for one or more Internet domains. If you are monitoring more than one Internet domain, you can use a description file instead of entering keyword strings in the Values tab in the Knowledge Script properties.

If you are using SMTPConnectivity, the account `a++++` is automatically added to the domain name for the test.

If you are using SMTPConnectivityEx, you must specify the account name, such as `a++++@abc.com` or `testaccount@def.com`.

The following parameters are used in the description file to determine the host status. You can specify these parameters at the beginning of the file (followed by a list of domain accounts) or after a single domain name:

- **UpSubject**. Type a keyword string that appears in the report subject line when the host is available.
- **DownSubject**. Type a keyword string that appears in the report subject line when the host is not available.
- **UpBody**. Type a keyword string that appears in the body of the report when the host is available.
- **DownBody**. Enter a keyword string that appears in the body of the report when the host is not available.

Note
If you do not specify a parameter, the parameter definition from the previous domain is used, if one was specified.

Here is a sample description file for **SMTPConnectivity** that uses the same Subject and Body keywords to check the `NetIQ Corporation` and `ABC` Internet domains:

```
UpSubject = “undelivered report”
DownSubject = “undelivered report”
UpBody = “user not found”
DownBody = “host not found”
[netiq.com]
[abc.com]
```

Here is a sample description file for SMTPConnectivityEx that describes three Internet domains. Note the use of the account names when using this script. The first domain (`netiq.com`) uses different keywords than the second domain (`abc.com`). The third domain (`def.com`) reuses the Subject and Body keywords from the second domain:

```
[a++++@netiq.com]
UpSubject = “undelivered report”
DownSubject = “undelivered report”
UpBody = “user not found”
DownBody = “host not found”

[testaccount@abc.com]
UpSubject = “delivery complete”
DownSubject = “non-delivered report”
UpBody = “delivery complete”
DownBody = “host unavailable”

[testaccouunt@def.com]
```

Checking Connectivity for Multiple Domains

To monitor more than one Internet domain and specify the host status parameters in the Values tab of the Knowledge Script properties dialog box, use only the specified keyword strings for each domain. The order in which you specify the keyword strings must correspond to the order in which you list the Internet domains, and you must use the pipe character (|) to separate the strings.

To monitor more than one Internet domain and specify the host status parameters in a description file rather than as a text string for each parameter, use the parameter definition for the previous domain. For more information, see “Understanding How Description Files Work” on page 1939.

SMTPConnectivityEx

Use this Knowledge Script to verify connectivity between an Exchange Server and one or more accounts at various Internet domains through an SMTP gateway. It does this by sending a message to a user account (either real or non-existent) and examining the resulting delivery report (DR) or non-delivery report (NDR).

This script scans the subject and body of the report for specific strings that indicate the status of the SMTP gateway host:

- If the test message is sent successfully to the SMTP host, and the message generates either a DR or an NDR, it indicates that the SMTP host is available and there is connectivity between Exchange and the SMTP gateway.
- If the test message generates an NDR because it fails to reach the SMTP host, it indicates that there is no connectivity between Exchange and the SMTP gateway.

Therefore, to configure this script, you need to know the strings that appear in the DR and NDR subject and body that indicate the delivery status.

If no report is received, it is interpreted as a connectivity failure.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

To use this Knowledge Script effectively, do the following before running this script:

1. Verify that your Exchange Server uses the Internet Mail Connector or Internet Mail Service to connect to the Internet through an SMTP gateway.
2. Verify the gateway forwards DRs to the mailbox associated with the AppManager agent service account as soon as they are received. If the AppManager agent mailbox does not receive DRs immediately, AppManager cannot accurately report the status of the SMTP host or the connectivity between the Exchange Server and the SMTP gateway.
3. If you do not allow NDRs, set up a user account for this script to use and ensure it sends a DR for successful deliveries.
4. As a test, send an e-mail message to both valid and invalid accounts on a valid domain and see how long it takes for the report to come back. If the report does not come back before the next time the script runs, it is interpreted as a connectivity failure.
5. If the AppManager agent mailbox successfully receives the DR, check the subject line and message body for the text strings that indicate the status of the SMTP server. The subject and body text in a DR can vary for each domain, but typically you can determine the status of the host by checking for the following information:
   - Check the subject line for a keyword string that indicates whether the test message was delivered. For example, `Delivered` means that the host is available, and the user exists. `Undeliverable` means either the host is unavailable, or the user does not exist, but you cannot tell which until you check the body. For each domain, identify the keywords that indicate the status of the server in the subject line.
   - Check the body of the message for a keyword string that indicates whether the test message was delivered. For example `Was delivered`. A text string such as `Destination server for this recipient could not be found` indicates no connectivity. A string such as `e-mail account does not exist` means that there is connectivity, even though there is no such account.

If the subject and the body of the DR do not help you to determine text strings to use for checking the availability of the SMTP host, try sending a test message to another domain.

6. To generate an NDR that indicates the host is down, send the test message when the domain is not available.

Note

This script requires the Exchange MO services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event for connectivity status. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns a value of 100 if the connection between the Exchange Server and Internet domain is up or a value of 0 if the connection is down during the interval. The detail message includes the name of each Exchange Server and domain connection checked. When there is connectivity, this Knowledge Script also collects the response time in seconds. The default is y.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange Server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange Server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Target domain account(s)	Specify the accounts at the domain names that you want to check. If specifying more than one, the order in which you specify the Internet domains must correspond to the list of Subject and Body Keywords. Use a pipe character (|) to separate multiple strings. For example: `a++++@abc.com|b++++@abc.com|a++++@xyz.com` The default domain account is a++++@netiq.com.
Subject keywords when ...	Provide a keyword string found in the subject line of the NDR message that indicates whether the host status is up or down. • **... host is up**. Enter a keyword string that appears in the subject line of the NDR when mail delivery fails but the host is available. The default is `Undeliverable`. • **... host is down**. Enter a keyword string that appears in the subject line of the NDR when mail delivery fails because the host is not available. The default keyword is `Undeliverable`. If specifying a string for more than one Internet domain, the order in which you specify the keyword strings must correspond to the list of Internet domains. Use a pipe character (|) to separate multiple strings. **Note** Depending on your environment, you may need to set keyword strings for both the subject line and the message body to determine the availability of the host server. For more information, see "Understanding How Keyword Strings Work" on page 1938. If you do not specify a value for a parameter, the parameter always matches. If you do not want to use a particular parameter to determine connectivity, you can enter a "garbage" string that does not appear in the NDR.
Body keywords when ...	Provide a keyword string found in the body of the NDR message that indicates whether the host status is up or down. • **... host is up**. Enter a keyword string that appears in the message body of the NDR when mail delivery fails but the host is available. The default message is `e-mail account does not exist`. • **... host is down**. Enter a keyword string that appears in the message body of the NDR when mail delivery fails because the host is not available. The default message is `destination server for this recipient could not be found`. If specifying a string for more than one Internet domain, the order in which you specify the keyword strings must correspond to the list of Internet domains. Use a pipe character (|) to separate multiple strings. **Note** Depending on your environment, you may need to set keyword strings for both the subject line and the message body to determine the availability of the host server. For more information, see "Understanding How Keyword Strings Work" on page 1938. If you do not specify a value for a parameter, the parameter always matches. If you do not want to use a particular parameter to determine connectivity, you can enter a "garbage" string that does not appear in the NDR.
Maximum threshold for a response	Specify the maximum number of seconds in which you expect to get a response. If a response takes longer than this number of seconds, this script raises an event. The default is 120 seconds.

Description	How to Set It
Description file on managed client	Set to **y** to use the keyword strings specified in a file on the managed client to describe the host status. If this parameter is set to y, the subject and body keywords are ignored. The default is n. For more information, see “Understanding How Description Files Work” on page 1939.

Description file name	Provide the full path to the file on the agent computer that contains the description file. For example:
	`C:\temp\msgsample.txt`
	To use the specified description file, you must set the Description file on managed client parameter to y.
	The default file name is `C:\temp\aa.txt`.
	You can use the UNC format to specify the path. For example:
	`\\ENG\appdev\mylog.txt`
	Tip You can only specify one file name for any job instance. To monitor multiple files, create separate Knowledge Script jobs.

Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event. The default is 5 (red event indicator).

SRSServiceDown

Use this Knowledge Script to monitor the status of the Site Replication Service (SRS). This script attempts to restart a service that is detected as down.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns 100 if the SRS service is running, 0 if the service is not running. The default is n.
Automatically re-start service?	Set to **y** to automatically restart the SRS service if it is down.
Event severity: Failed to restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SRS service is down and AppManager cannot restart the service. The default is 5 (red event indicator).
Event severity: Successful restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SRS service is down and AppManager restarted the service. The default is 25 (blue event indicator).
Event severity: Do not restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SRS service is down and you do not want to restart the service. The default is 18 (yellow event indicator).

TopNISMailboxRes

Use this Knowledge Script to monitor the file space used by the top private information store folders or mailboxes. This script raises an event if the file space for a specified number of mailboxes or folders exceeds the threshold you set.

If a failover occurs while this Knowledge Script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the file space (in MB) used by the top *n* number of folders or mailboxes combined. The default is n.
Monitor the top N mailboxes	Specify the number of top mailboxes you want to monitor. For example, to see the five mailboxes that use the most file space, enter 5. The default is 10. Enter 0 to include all mailboxes.
Maximum threshold for file space size (MB)	Specify the maximum file space size that private information store mailboxes can have before an event is raised. The default is 300 MB.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Character to separate fields in detail message	Provide a character or string of characters to separate each field of data in the event detail message and graph data details. The default character, Null, specifies a Tab character which represents a fixed column width defined within the Knowledge Script.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

TopNISPublicRes

Use this Knowledge Script to monitor the file space used by the top public information store folders (public folders). This script raises an event if the file space for a specified number of public folders exceeds the threshold you set.

Note

This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the total file space used by the top *n* number of folders. The default is n.
Monitor top N folders	Specify the number of top public folders you want to monitor. For example, to see the five folders that use the most file space, enter 5. The default value is 10. Enter 0 to include all public folders.
Maximum threshold for file space size (MB)	Specify the maximum file space size that public information store folders can have before an event is raised. The default is 300 MB.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Character to separate fields in detail message	Provide a character or string of characters to separate each field of data in the event detail message and graph data details. The default character, Null, specifies a Tab character which represents a fixed column width defined within the Knowledge Script.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

TopNReceivers

Use this Knowledge Script to monitor which users received the most mail messages and the total file size of mail messages received by the top users or all users. You can specify the number of top users and the tracking period for when mail messages have been received.

To use this script, you must enable tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages received if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. This script adjusts for your time zone.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of mail messages received by the top *n* number of users. The default option is n. **Hint** To collect data to display in the Report_TopNReceivers report, also enable data detail archiving: 1. On the **Advanced** tab, ensure the **Do not archive data detail** option is not selected. 2. Click **OK**.
Detail level (0-2) for event detail message	Specify the level of information that you want to include in the event detail message. The default is 0 which includes the total file size of all messages received by a user. Additional information is available by specifying a detail level: • **0** monitors total file size of messages • **1** monitors the number of messages • **2** monitors file size and number of messages. The default is 2.
Maximum threshold for total file size (MB)	Specify the maximum file size that all messages can have before an event is raised. The default is 300 MB.

Description	How to Set It
Maximum threshold for total number of messages	Specify maximum number of messages that can exist before an event is raised. The default is 1000 messages.
Monitor top N receivers	Specify the number of top users you want to monitor. For example, to see the five users who have received the most e-mail in the period, enter 5. The default value is 3.
Count past N days (including today)	Specify the number of days to use as a tracking period. The default value is 5 (the past 4 days plus today). If you set this value higher than the actual number of daily tracking logs available, the value is reset to the actual number of daily logs. For example, if you set the value to 8 but there are only 5 daily logs available, the value is changed to 5.
Character to separate fields in detail message	Provide a character or string of characters to separate each field of data in the event detail message and graph data details. The default character, Null, specifies a Tab character which represents a fixed column width defined within the Knowledge Script.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

TopNSenders

Use this Knowledge Script to monitor which users sent the most mail messages recently. This script monitors the total file size of mail messages sent by the top users or all users. You can specify the number of top users and the tracking period for when mail messages have been sent.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages sent if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. This script adjusts for your time zone.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of mail messages sent by the top *n* number of users. The default option is n. **Hint** To collect data to display in the Report_TopNSenders report, also enable data detail archiving: 1. On the **Advanced** tab, ensure the **Do not archive data detail** option is not selected. 2. Click **OK**.
Detail level (0-2) for event detail message	Specify the level of information that you want included in the event detail message. The default specifies the total file size of all messages sent by a user. Additional information is available by specifying a detail level: • **0** monitors total file size of messages • **1** monitors the number of messages • **2** monitors file size and number of messages. The default value is 2.
Maximum threshold for total file size	Specify the maximum size that sent files can attain before an event is raised. The default is 300 MB.

Description	How to Set It
Maximum threshold for total number of messages	Specify the maximum number of messages that can be sent before an event is raised. The default is 1000 messages.
Monitor top N senders	Specify the number of top users you want to monitor. For example, to see the five users who have sent the most e-mail in the period, enter 5. The default value is 3.
Count past N days (including today)	Specify the number of days to use as a tracking period. The default value is 5 (the past 4 days plus today). If you set this value higher than the actual number of daily tracking logs available, the value is reset to the actual number of daily logs. For example, if you set the value to 8 but there are only 5 daily logs available, the value is changed to 5.
Character to separate fields in detail message	Specify a character or string of characters to separate each field of data in the event detail message and graph data details. The default character, Null, specifies a Tab character which represents a fixed column width defined within the Knowledge Script.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

Chapter 35
Exchange 2007 Knowledge Scripts

AppManager for Exchange Server 2007 and 2010 provides Knowledge Scripts for monitoring Microsoft Exchange Server 2007 and 2010.

The Exchange Server 2007 Knowledge Scripts supports Microsoft Exchange Server 2007 resources installed in *non-clustered* environments and the following *clustered* environments:

- *Cluster continuous replication* (CCR) combines the log shipping and replay functionality in Exchange Server 2007 with the failover functionality in the Microsoft cluster service. CCR is a solution that can be deployed with no single point of failure in a single datacenter or between two datacenters.
- *Single copy clusters* (SCC), known as shared storage clusters in previous versions of Exchange Server, are present in Exchange Server 2007.

In a clustered environment, AppManager raises error events if failover occurs while jobs are running. These error events are expected results of the failover process and can be safely ignored.

A subset of the Knowledge Scripts support Microsoft Exchange Server 2010 resources installed in a database availability group (DAG). A DAG is a set of up to 16 Microsoft Exchange Server 2010 Mailbox servers that provides automatic database-level recovery from a database, server, or network failure. Exchange Server 2010 does not use storage groups.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
All_BestPracticesAnalyzer	Monitors the Windows event log for errors and warnings raised by the Exchange Best Practices Analyzer.
All_ClockSynchronization	Monitors the synchronization of clocks for one or more Domain Controllers.
All_EventLog	Monitors the Windows Application event log for errors and warning events related to Exchange Server 2007 and 2010.
All_ServiceStatus	Monitors the status of Exchange Server 2007 and 2010 services.
CAS_Activity	Monitors Client Access server services and functions.
CAS_Connectivity	Monitors connectivity for Client Access server services: ActiveSync, Outlook Web Access, Outlook Web services, and the Autodiscover service.
CAS_OABAvailability	Monitors whether offline address books can be downloaded.
CAS_PublicFolderAvailability	Monitors the accessibility of public folders on the Client Access server.
ETS_ExternalMail	Monitors e-mail sent to and from your Exchange environment.

Knowledge Script	What It Does
ETS_MessageHygiene	Monitors message hygiene functions for the Edge Transport server.
HTS_Connectivity	Monitors the status of send, receive, and foreign connectors, monitors connectivity with a Mailbox server, and monitors the time of the last synchronization with the Edge Transport server.
HTS_SendersAndRecipients	Measures number of messages in a mailbox and total message size for senders and recipients.
HTS_TransportDumpster	Monitors Transport Dumpster activity, availability, and the number of items in the Transport Dumpster.
MBS_ClusterOwner	Determines whether an Exchange Server is the owner of the node and whether the CMS is down. This script only runs on servers with Exchange Server 2007.
MBS_DatabaseStateChange	Monitors changes in the state of mailbox databases on an Exchange Server. States include active, passive, suspended, removed, or unmounted.
MBS_DatabaseStatus	Monitors Exchange Server 2007 and 2010 mailbox databases for size of online maintenance window, defragmentation time, free log space, free file space, and number of mailboxes.
MBS_MailboxAccessibility	Monitors the ability of the Mailbox server to access individual mailboxes.
MBS_MailboxUsage	Measures the size of mailboxes by the number of messages in the mailbox or by total message size in MB.
MBS_MailFlow	Sends test e-mail to local or remote Mailbox servers.
MBS_MessagingRecordsMgmt	Monitors message management tasks such as deleting, journaling, moving, and retention.
MBS_PublicFolderUsage	Measures the size of public folders by the number of messages in the folders or by total message size in MB.
MBS_Replication	Monitors replication status and performance for a Mailbox server.
Transport_BackPressure	Monitors the status of back pressure for the Hub Transport server.
Transport_QueueStatus	Monitors the status of queues on the Hub Transport server: submission queue, mailbox delivery queue, remote delivery queue, poison message queue, and unreachable destination queue.
UMS_CallActivity	Monitors call activity on the Unified Messaging server: voice, fax, play on phone, auto attendant, subscriber access, prompt editing.
UMS_Connectivity	Monitors connectivity to Hub Transport servers, Mailbox servers, Active Directory, and Unified Messaging-enabled mailboxes.
UMS_Failures	Monitors failures related to redirected calls, disconnected calls, and access to Active Directory, the Hub Transport server, and the Mailbox server.
UMS_Performance	Monitors the performance of the Unified Messaging server: user response latency, operation response time, queued messages for call answering, queued OCS user notifications, and calls disconnected while playing audio hourglass tones.
Recommended Knowledge Script Group	Performs essential monitoring of your Exchange Server 2007 or 2010 environment.

All_BestPracticesAnalyzer

Use this Knowledge Script to monitor the Windows event log for errors and warnings whose source is BPA (Exchange Best Practices Analyzer). This script raises an event if the Knowledge Script job fails or the event log contains error and warning messages.

If you are not running the BPA, you can use this script to execute the BPA each time the script runs. If you set the *Execute Best Practices Analyzer during job?* parameter to **Yes**, AppManager runs the BPA at each iteration of the Knowledge Script job. AppManager then stops the BPA and analyzes the event log for errors and warnings raised by the BPA.

Notes

- This script may raise duplicate events on computers where multiple Exchange Server 2007 and 2010 roles are installed. These duplicate events are raised because the BPA populates the event log with errors and warnings for *each role* when the error or warning is applicable for the entire Exchange Server 2007 or 2010 organization.
- Most BPA events do not indicate which role they are associated with. Therefore, this script raises events that are not associated with a role. However, the AppManager event messages include the text of the BPA event, which should help you determine which role is affected.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Running the ExBPAcmd.exe Tool Manually

The BPA must be running so that it can submit any errors or warnings to the event log. This script will not work if you are not running the BPA and do not enable the *Execute Best Practices Analyzer during job?* parameter.

If you do not enable this script to launch the BPA, then run the `ExBPAcmd.exe` tool manually to monitor the Windows Event Log for errors and warnings.

To run the ExBPAcmd.exe tool manually:

1. Open the Exchange Management Shell.
2. Run the following command:

   ```
   $exBPAoutput = . "C:\Program Files\Microsoft\Exchange Server\Bin\ExBPAcmd.exe" -
   p Events:Enable -r "5,$role,$scan_type,Server=<ExchangeServerName>"
   ```

   where `$role` is one of the following values enclosed in quotation marks (" "): `Mailbox`, `Gateway`, `Bridgehead`, `ClientAccess`, `ClusterMailbox`

   where `$scan_type` is one of the following values enclosed in quotation marks (" "): `Health`, `ConnectivityTask`, `Ex2007Readiness`, `Perf`, `Permissions`

   where `<ExchangeServerName>` is the name of the Exchange server where you want to run the `ExBPAcmd.exe` tool.
3. Run the following command to display the output of the `ExBPAcmd.exe` tool:

   ```
   Write-Host $exBPAoutput
   ```

   These commands enable the event log register.

Prerequisites

Before running this script, ensure that the following permissions and memberships exist.

Component	Required Permissions and Memberships
Account running the AppManager agent service (netiqmc)	• Membership in the Builtin\Administrators group on the Active Directory server • Membership in the local Administrators group on the local computer • Delegation for at least Exchange View-Only permissions
Exchange Best Practice Analyzer tool (for all Exchange Server roles)	• Designation as the Domain Administrator, or membership in the Builtin\Administrators group on the Active Directory server, for enumerating the Active Directory information and calling the Microsoft Windows Management Instrumentation (WMI) providers on the domain controller and global catalog servers • Membership in the Local Administrators group on each Exchange server for calling the WMI providers and accessing the registry and the metabase • Delegation for at least Exchange View-Only Permissions on the Exchange organization

Resource Object

Exchange_Server

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the All_BestPracticesAnalyzer job fails. The default is 5.
Analyze Exchange Server 2007/2010 Best Practices	
Execute Best Practices Analyzer during job?	Select **Yes** to allow AppManager to launch the BPA using a command-line execution of `ExBPACmd.exe` at each iteration of this script. If you are already running the BPA, then clear this option. The BPA *must* be running so that it can submit any errors or warnings to the event log. The default is Yes.

Parameter	How to Set It
Type of scan to execute	Select the type of scan the BPA should perform: • **Connectivity Test**. To scan network connections and permissions for the selected Exchange server. • **Exchange 2007 Readiness Check**. To assess your organization's readiness for Exchange Server 2007. • **Health Check**. To perform a full scan, checking for errors, warnings, and configuration information. This option is selected by default. • **Permission Check**. To ensure that your Exchange Server 2007 deployment has the proper credentials as defined by your organization.
Event Notification	
Comma-separated list of event IDs to ignore	Provide a list of error and warning ID numbers that this script should ignore when scanning the event log. Separate the numbers with a comma.
Raise event for errors found in Windows Event Log?	Select **Yes** to raise an event when the event log contains error messages raised by the BPA. The default is Yes.
Event severity when errors found in the Windows Event Log	Set the severity level, from 1 to 40, to indicate the importance of an event in which the event log contains error messages. The default is 5.
Raise event for warnings found in Windows Event Log?	Select **Yes** to raise an event when the event log contains warning messages raised by the BPA. The default is Yes.
Event severity for warnings found in the Windows Event Log	Set the severity level, from 1 to 40, to indicate the importance of an event in which the event log contains warning messages raised by the BPA. The default is 15.

All_ClockSynchronization

Use this Knowledge Script to monitor the synchronization of clocks for one or more Domain Controllers. This script raises an event if the number of seconds of difference between clocks exceeds the threshold you set.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Resource Object

Exchange_Server

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the All_ClockSynchronization job fails. The default is 5.
Monitor Clock Synchronization with Domain Controller	
Comma-separated list of Domain Controllers to test	Use this parameter to limit the number of Domain Controller (DC) clocks that are tested for synchronization with the clock on the server running the ClockSynchronization Knowledge Script. Provide a list of fully qualified hostnames, separating multiple names by commas. Leave this parameter blank to test all DC clocks in your organization.
Event Notification	
Raise event if clocks are not synchronized?	Select **Yes** to raise an event if the clock on the server running the ClockSynchronization Knowledge Script is not synchronized with the clock on the DC. The default is Yes.
Threshold - Maximum clock difference	Set the maximum number of seconds that the server clock can be out of sync with the DC. For example, setting the threshold to 2 indicates that it is acceptable for the clock to be two seconds faster or slower than the clock on the DC. The default is 10 seconds. If you want the server clock to be in sync with the DC clock, set this parameter to 0.
Event severity when clock difference exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the clock synchronization offset exceeds the threshold you set. The default is 25.

All_EventLog

Use this Knowledge Script to monitor the Windows Application event log for errors and warnings that contain the word **exchange**. This script raises an event if event log entries match your search criteria. You can filter your search by event ID, event category, and event source.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Resource Object

Exchange_Server

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the All_EventLog job fails. The default is 5.
Monitor Windows Event Log	
Event Notification	
Comma-separated list of event sources to ignore	Provide a list of event sources that this script should ignore when scanning the Application event log. Separate the source names with a comma. Event sources are computers whose names are displayed in the Source column of the event log.
Comma-separated list of event categories to ignore	Provide a list of event categories that this script should ignore when scanning the Application event log. Separate the category names with a comma.
Comma-separated list of event IDs to ignore	Provide a list of error and warning ID numbers that this script should ignore when scanning the Application event log. Separate the numbers with a comma.
Raise event if Exchange error events are found?	Select **Yes** to raise an event if the Application event log contains error events that match your search criteria. The default is Yes.
Event severity when Exchange error events are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Application event log contains error events. The default is 10.
Raise event if Exchange warning events are found?	Select **Yes** to raise an event if the Application event log contains warning events that match your search criteria. The default is Yes.
Event severity when Exchange warning events are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Application event log contains warning events. The default is 20.

All_ServiceStatus

Use this Knowledge Script to monitor the status of Exchange Server 2007 and 2010 services. This script raises an event when services are not running and when stopped services fail to start.

This script monitors and restarts the following Exchange Server 2007 and 2010 services:

Mailbox Server Role Services		
Monitoring	Active Directory Topology	Information Store
Mailbox Assistants	Mail Submission	Replication Service
System Attendant	Search Indexer	Service Host
Transport Log Search	Search (Exchange)	Server Extension for Windows Server Backup
Client Access Server Role Services		
Service Host	Active Directory Topology	File Distribution
Hub Transport Server Role Services		
Active Directory Topology	EdgeSync	Transport
Transport Log Search		
Edge Transport Server Role Services		
ADAM	Credential Service	Transport
Anti-SPAM Update	Monitoring	Transport Log Search
Unified Messaging Server Role Services		
Active Directory Topology	File Distribution	Monitoring
Unified Messaging	Speech Engine	

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Resource Objects

- Exchange2007_Services
- Exchange2007_Service
- Exchange2010_Services
- Exchange2010_Service

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the All_ServiceStatus job fails. The default is 5.
Monitor Status of Exchange 2007/2010 Services	
Services to be Monitored	
Monitor services configured to start automatically?	Select **Yes** to monitor Exchange Server 2007 and 2010 services that are configured to start automatically. The default is Yes. When you enable this parameter, the All_ServiceStatus job does not raise events for services that are configured to start manually, nor does it start manual services that are not running.
Monitor services configured to start manually?	Select **Yes** to monitor Exchange Server 2007 and 2010 services that are configured to start manually. The default is No. When enabled, the All_ServiceStatus job does not raise events for services that are configured to start automatically.
Event Notification	
Raise event if Exchange 2007/ 2010 services are not running?	Select **Yes** to raise an event if at least one Exchange Server service is not running. The default is Yes. When you enable this parameter, the All_ServiceStatus job raises events only for those services you selected in the **Services to be Monitored** parameters.
Event severity when services are not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which at least one Exchange Server service is not running. The default is 10.
Start services not currently running?	Select **Yes** to start Exchange Server 2007 or 2010 services that are not running. The default is Yes. When you enable this parameter, the All_ServiceStatus job starts only those services you selected in the **Services to be Monitored** parameters.
Threshold - Timeout for service startup	Set the number of seconds that AppManager should wait for Exchange Server 2007 or 2010 services to restart before raising an event. The default is 60 seconds.
Raise event if stopped services fail to start?	Select **Yes** to raise an event if AppManager cannot start Exchange Server services that are not running. The default is Yes.
Event severity when stopped services fail to start	Set the severity level, from 1 to 40, to indicate the importance of an event in which Exchange Server services fail to start after the specified timeout period. The default is 5.

CAS_Activity

Use this Knowledge Script to monitor Client Access server services and functions:

- Availability Service activity
- ActiveSync response time and request rate
- Outlook Web Access response time, search time, login rate, and login failures
- Outlook Web Services request rate and current connections
- IMAP4 (Internet Message Access protocol) processing time, current connections, and active SSL connections
- POP3 (Post Office Protocol) processing time, login rate, current connections, and active SSL connections

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Resource Objects

- Exchange2007_ClientAccessServer
- Exchange2010_ClientAccessServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CAS_Activity job fails. The default is 5.
Monitor Availability Service Activity	
Event Notification	
Raise event if response time for free/busy requests exceeds threshold?	Select **Yes** to raise an event if the response time for free and busy requests to Microsoft Outlook exceeds the threshold you set. The default is Yes. The Availability Service monitors free/busy requests.
Threshold - Maximum free/busy request response time	Set the maximum length of time that Microsoft Outlook can take to respond to free/busy requests before an event is raised. The default is 5000 milliseconds.
Event severity when response time for free/busy requests exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the response time for free/busy requests exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for free/busy request response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the length of response time during the monitoring interval. The default is No.
Monitor ActiveSync Activity	
Monitor ActiveSync Response Time	
Event Notification	
Raise event if ActiveSync response time exceeds threshold?	Select **Yes** to raise an event if the response time for ActiveSync exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time	Set the maximum length of time that ActiveSync can take to respond to requests before an event is raised. The default is 100 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which ActiveSync response time exceeds the threshold. The default is 15.
Data Collection	
Collect data for response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the length of response time during the monitoring interval. The default is No.
Monitor ActiveSync Request Rate	
Event Notification	
Raise event if ActiveSync request rate exceeds threshold?	Select **Yes** to raise an event if the rate of synchronization requests to ActiveSync exceeds the threshold you set. The default is Yes.
Threshold - Maximum request rate	Set the maximum number of requests that can occur per second before an event is raised. The default is 10 synchronization requests per second.
Event severity when request rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ActiveSync request rate exceeds the threshold. The default is 15.
Data Collection	
Collect data for request rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate of synchronization requests during the monitoring interval. The default is No.
Monitor Outlook Web Access Activity	
Monitor Outlook Web Access Response Time	
Event Notification	
Raise event if Outlook Web Access response time exceeds threshold?	Select **Yes** to raise an event if the response time for Outlook Web Access (OWA) exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time	Set the maximum amount of time that it can take for OWA to respond to requests before an event is raised. The default is 100 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which OWA response time exceeds the threshold. The default is 15.
Data Collection	
Collect data for response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the length of response time during the monitoring interval. The default is No.
Monitor Outlook Web Access Search Time	
Event Notification	

Parameter	How to Set It
Raise event if Outlook Web Access search time exceeds threshold?	Select **Yes** to raise an event if Outlook Web Access (OWA) search time exceeds the threshold. The default is Yes. The OWA search feature allows users to find items in a mailbox.
Threshold - Maximum search time	Set the maximum length of time that OWA can spend performing a search before an event is raised. The default is 100 milliseconds.
Event severity when search time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which OWA search time exceeds the threshold. The default is 15.
Data Collection	
Collect data for search time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the length of search time during the monitoring interval. The default is No.
Monitor Outlook Web Access Login Rate	
Event Notification	
Raise event if login rate exceeds threshold?	Select **Yes** to raise an event if the rate at which users log in to Outlook Web Access (OWA) exceeds the threshold. The default is Yes.
Threshold - Maximum login rate	Set the maximum rate at which users can log in to OWA before an event is raised. The default is 10 logins per second.
Event severity when login rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the rate at which users log in to OWA exceeds the threshold. The default is 15.
Data Collection	
Collect data for login rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the OWA log in rate for the monitoring interval. The default is No.
Monitor Outlook Web Access Login Failures	
Event Notification	
Raise event if login failures exceed threshold?	Select **Yes** to raise an event if the failures for logging in to Outlook Web Access (OWA), expressed as a percentage of all login attempts, exceed the threshold. The default is Yes.
Threshold - Maximum percentage of login failures	Set the maximum percentage of OWA login failures that can occur before an event is raised. The default is 10%.
Event severity when login failures exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which percentage of OWA login failures exceeds the threshold. The default is 15.
Data Collection	
Collect data for login failures?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of OWA login failures for the monitoring interval. The default is No.
Monitor Outlook Web Services Activity	
Monitor Outlook Web Services Request Rate	
Event Notification	
Raise event if Outlook Web Services request rate exceeds threshold?	Select **Yes** to raise an event if the rate of requests to Outlook Web Services exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum request rate	Set the maximum number of requests that can occur per second before an event is raised. The default is 10 requests per second.
Event severity when request rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the rate of requests to Outlook Web Services exceeds the threshold. The default is 15.
Data Collection	
Collect data for request rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate of requests during the monitoring interval. The default is No.
Monitor Outlook Web Services Current Connections	
Event Notification	
Raise event if number of current connections exceeds threshold?	Select **Yes** to raise an event if the number of connections established with Outlook Web Services exceeds the threshold you set. The default is Yes. By knowing the number of current connections, you can determine user load for Outlook Web Services.
Threshold - Maximum number of current connections	Set the maximum number of connections to Outlook Web Services that can be established before an event is raised. The default is 25 connections.
Event severity when number of current connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of connections established with Outlook Web Services exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of current connections?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of connections established during the monitoring interval. The default is No.
Monitor IMAP4 Activity	
Monitor IMAP4 Command Processing Time	
Event Notification	
Raise event if command processing time exceeds threshold?	Select **Yes** to raise an event if the amount of processing time for IMAP4 commands exceeds the threshold you set. The default is Yes.
Threshold - Maximum command processing time	Set the maximum amount of time that can be spent processing IMAP4 commands before an event is raised. The default is 100 milliseconds.
Event severity when command processing time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the amount of processing time for IMAP4 commands exceeds the threshold. The default is 15.
Data Collection	
Collect data for command processing time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the amount of processing time spent during the monitoring interval. The default is No.
Monitor IMAP4 Current Connections	
Event Notification	
Raise event if number of current connections exceeds threshold?	Select **Yes** to raise an event if the number of current IMAP4 connections to your Exchange server exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of current connections	Set the maximum number of IMAP4 connections that can be established before an event is raised. The default is 10 connections.

Parameter	How to Set It
Event severity when number of current connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of IMAP4 connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of current connections?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of IMAP4 connections established during the monitoring interval. The default is No.
Monitor IMAP4 Active SSL Connections	
Event Notification	
Raise event if number of active SSL connections exceeds threshold?	Select **Yes** to raise an event if the number of current IMAP4 connections to your Exchange server over SSL (Secure Sockets Layer) exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of active SSL connections	Set the maximum number of IMAP4 connections that can be established over SSL before an event is raised. The default is 50 connections.
Event severity when number of active SSL connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of IMAP4 SSL connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of active SSL connections?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of IMAP4 SSL connections established during the monitoring interval. The default is No.
Monitor POP3 Activity	
Monitor POP3 Command Processing Time	
Event Notification	
Raise event if command processing time exceeds threshold?	Select **Yes** to raise an event if the amount of processing time for POP3 commands exceeds the threshold you set. The default is Yes.
Threshold - Maximum command processing time	Set the maximum amount of time that can be spent processing POP3 commands before an event is raised. The default is 10 milliseconds.
Event severity when command processing time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the amount of processing time for POP3 commands exceeds the threshold. The default is 15.
Data Collection	
Collect data for command processing time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the amount of processing time spent during the monitoring interval. The default is No.
Monitor POP3 Login Rate	
Event Notification	
Raise event if login rate exceeds threshold?	Select **Yes** to raise an event if the rate at which users log in to Exchange over POP3 exceeds the threshold you set. The default is Yes.
Threshold - Maximum login rate	Set the maximum number of POP3 login requests that can occur per second before an event is raised. The default is 10 logins per second.
Event severity when login rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of POP3 login requests exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for login rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of POP3 login requests for the monitoring interval. The default is No.
Monitor Current POP3 Connections	
Event Notification	
Raise event if number of current connections exceeds threshold?	Select **Yes** to raise an event if the number of current POP3 connections to your Exchange server exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of current connections	Set the maximum number of POP3 connections that can be established before an event is raised. The default is 10 connections.
Event severity when number of current connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of POP3 connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of current connections?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of POP3 connections established during the monitoring interval. The default is No.
Monitor POP3 Active SSL Connections	
Event Notification	
Raise event if number of active SSL connections exceeds threshold?	Select **Yes** to raise an event if the number of current POP3 connections to your Exchange server over SSL (Secure Sockets Layer) exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of active SSL connections	Set the maximum number of POP3 connections that can be established over SSL before an event is raised. The default is 25 connections.
Event severity when number of active SSL connections exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of POP3 SSL connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of active SSL connections?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of POP3 SSL connections established during the monitoring interval. The default is No.

CAS_Connectivity

Use this Knowledge Script to monitor the connectivity of Client Access server services: ActiveSync, Outlook Web Access, Outlook Web services, and the Autodiscover service. This script raises an event when a connectivity test fails and when response time exceeds the threshold you set.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026

When you run the CAS_Connectivity Knowledge Script on a Client Access Server, the script automatically creates a CAS test user mailbox on each Mailbox server in the Exchange deployment if those mailboxes do not already exist. In an Exchange deployment containing both Exchange 2007 and Exchange 2010 servers, if you run the CAS_Connectivity script on an Exchange 2010 Client Access Server, the script will not be able to create the mailboxes on Exchange 2007 Mailbox Servers, and AppManager raises an error event about the problem. In this situation, you must manually create the CAS test user mailboxes on the Exchange 2007 Mailbox Servers.

To create CAS test user mailboxes on an Exchange 2007 Mailbox Server:

1. Log in to one of the Exchange 2007 Mailbox Servers and open the Exchange Management Shell.
2. Change directories to the `Scripts` directory, located under the Microsoft Exchange installation directory.
3. Run the following command:
   `Get-MailboxServer | .\New-TestCasConnectivityUser.ps1`.
4. Follow the on-screen instructions to create the CAS test user mailbox on each Mailbox server.

Resource Objects

- Exchange2007_ClientAccessServer
- Exchange2010_ClientAccessServer

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Communicate only with Exchange Servers in the local domain?	Select **Yes** to test only Exchange Servers in the same domain as the server on which you run the CAS_Connectivity job. When this option is unselected, certain tests for the Client Access server attempt to contact *all* Mailbox servers in your organization. These tests will fail if the Exchange accounts in one domain do not have access to other domains. Leave this option unselected if you specify a Mailbox server in the *Mailbox server to be used for connectivity tests* parameter.

Parameter	How to Set It
Ignore these Mailbox servers when testing CAS to MBS communications	Provide a comma-separated list of the hostnames of the Mailbox servers that you want to exclude from connectivity testing between the Client Access server and the Mailbox server. Leave this option blank if you specify a Mailbox server in the *Mailbox server to be used for connectivity tests* parameter.
Mailbox server to be used for connectivity tests	By default, the CAS_Connectivity job tests connectivity to all Mailbox servers. Use this parameter to enable testing to one Mailbox server. Enter the hostname of the computer that hosts the Mailbox server with which you want to check connectivity. The hostname need not be fully qualified unless DNS lookup does not resolve the simple name.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CAS_Connectivity job fails. The default is 5.
Monitor ActiveSync Connectivity	
Event Notification	
Raise event if ActiveSync connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to ActiveSync. The default is Yes.
Event severity when ActiveSync connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to ActiveSync. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to ActiveSync exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for connectivity test	Set how long AppManager should wait for connectivity with ActiveSync before raising an event. The default is 10000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time it takes to connect to ActiveSync exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for ActiveSync response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average response time for connecting to ActiveSync. The default is No.
Monitor Outlook Web Access Connectivity	
URL type to be used for connectivity test	Select whether you want to use an internal or an external URL for the connectivity test. The default type is Internal.
Event Notification	
Raise event if Outlook Web Access connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to Outlook Web Access (OWA). The default is Yes.
Event severity when Outlook Web Access connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to OWA. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to Outlook Web Access exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for connectivity test	Set how long AppManager should wait to confirm connectivity with OWA before raising an event. The default is 10000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time it takes to connect to OWA exceeds the threshold that you set. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for Outlook Web Access response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average response time for connecting to OWA. The default is No.
Monitor Outlook Web Services Connectivity	
Use SSL (HTTPS) for connectivity test?	Select **Yes** to use Secure Socket Layer (SSL) to test connectivity to Outlook Web services. The default is No. If you select **Yes**, AppManager will use only SSL to test connectivity. If you clear the option, AppManager will first use SSL to test connectivity. If that attempt fails, AppManager will then try to test connectivity without using SSL.
Event Notification	
Raise event if Outlook Web services connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to Outlook Web services. The default is Yes.
Event severity when Outlook Web services connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to Outlook Web services. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to Outlook Web services exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for connectivity test	Set how long AppManager should wait to confirm connectivity with Outlook Web services before raising an event. The default is 10000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time taken for testing connectivity to Outlook Web services exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for Outlook Web services response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average response time for connecting to Outlook Web services. The default is No.
Monitor Autodiscover Service Connectivity	
Event Notification	
Raise event if Autodiscover service connectivity test fails?	Select **Yes** to raise an event if AppManager cannot check connectivity to the Autodiscover service. The default is Yes. The Autodiscover service allows Outlook 2007 clients and mobile devices to be recognized when they connect to the Client Access server.
Event severity when Autodiscover service connectivity test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot check connectivity to the Autodiscover service. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to the Autodiscover service exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for connectivity test	Set how long AppManager should wait to confirm connectivity with the Autodiscover service before raising an event. The default is 10000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time taken for testing connectivity to the Autodiscover service exceeds the threshold that you set. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for Autodiscover service response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average response time for connecting to the Autodiscover service. The default is No.

CAS_OABAvailability

Use this Knowledge Script to monitor the availability of offline address books (OABs) for a Client Access server. This script raises an event if OABs cannot be downloaded.

Resource Objects

- Exchang2007_ClientAccessServer
- Exchange2010_ClientAccessServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Communicate only with Exchange Servers in the local domain?	Select **Yes** to test only Exchange Servers in the same domain as the server on which you run the OABAvailability job. When this option is unselected, certain tests for the Client Access server attempt to contact *all* Mailbox servers in your organization. These tests will fail if the Exchange accounts in one domain do not have access to other domains. Leave this option unselected if you specify a Mailbox server in the *Mailbox server hosting offline address books to be accessed* parameter.
Ignore these Mailbox servers when testing CAS to MBS communications	Provide a comma-separated list of the hostnames of the Mailbox servers that you want to exclude from availability testing between the Client Access server and the Mailbox server. Leave this option blank if you specify a Mailbox server in the *Mailbox server hosting offline address books to be accessed* parameter.
Mailbox server hosting offline address books to be accessed	By default, the OABAvailability job tests connectivity to all Mailbox servers. Use this parameter to enable testing to one Mailbox server. Enter the hostname of the Mailbox server computer that hosts the OABs you want to monitor. The hostname need not be fully qualified unless DNS lookup does not resolve the simple name.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OABAvailability job fails. The default is 5.
Monitor Offline Address Book Availability	
Event Notification	
Raise event if offline address books cannot be downloaded?	Select **Yes** to raise an event if the Client Access server's offline address books cannot be downloaded. The default is Yes.
Event severity when offline address books cannot be downloaded	Set the severity level, from 1 to 40, to indicate the importance of an event in which offline address books cannot be downloaded. The default is 5.

CAS_PublicFolderAvailability

Use this Knowledge Script to monitor the accessibility of public folders on a Client Access server. This script raises an event when public folders are inaccessible.

Resource Objects

- Exchange2007_ClientAccessServer
- Exchange2010_ClientAccessServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Communicate only with Exchange Servers in the local domain?	Select **Yes** to test only Exchange Servers in the same domain as the server on which you run the CAS_PublicFolderAvailability job. When this option is unselected, certain tests for the Client Access server attempt to contact *all* Mailbox servers in your organization. These tests will fail if the Exchange accounts in one domain do not have access to other domains. Leave this option unselected if you specify a Mailbox server in the *Mailbox server hosting public folders to be accessed* parameter.
Ignore these Mailbox servers when testing CAS to MBS communications	Provide a comma-separated list of the hostnames of the Mailbox servers that you want to exclude from availability testing between the Client Access server and the Mailbox server. Leave this option blank if you specify a Mailbox server in the *Mailbox server hosting public folders to be accessed* parameter.
Mailbox server hosting public folders to be accessed	By default, the CAS_PublicFolderAvailability job tests connectivity to all Mailbox servers. Use this parameter to enable testing to one Mailbox server. Enter the hostname of the Mailbox server computer that hosts the public folders you want to monitor. The hostname need not be fully qualified unless DNS lookup does not resolve the simple name.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CAS_PublicFolderAvailability job fails. The default is 5.
Monitor Public Folder Availability	
Event Notification	
Raise event if public folders are inaccessible?	Select **Yes** to raise an event if the public folders on the Client Access server are inaccessible. The default is Yes.
Event severity when public folders are inaccessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which public folders on the Client Access server are inaccessible. The default is 5.

ETS_ExternalMail

Use this Knowledge Script to monitor e-mail sent to and from your Exchange environment. This script raises an event when average mail volume for recipients, recipient domains, senders, and sending domains exceeds the threshold you set. You select whether mail volume is measured by number of messages or total size of messages in MB.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Resource Objects

- Exchange2007_EdgeTransportServer
- Exchange2010_EdgeTransportServer

Default Schedule

By default, this script runs daily.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Measure mail volume by message count or total message size	Select how this script measures the volume of mail sent to and from your Exchange environment. Choose from **Message count** or **Total message size**. Total message size is measured in MB.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ETS_ExternalMail job fails. The default is 5.
Monitor Recipient Domains of Outgoing Mail	
Number of top recipient domains of outgoing mail	Set the top *n* recipient domains to be monitored for average mail volume. The default is 10 domains, the minimum is 0, and the maximum is 2147483647. To monitor all recipient domains for average mail volume, enter 0.
Event Notification	
Raise event if average mail volume for top recipient domains exceeds threshold?	Select **Yes** to raise an event if the average mail volume for the top *n* recipient domains exceeds the threshold you set. The default is Yes.
Threshold - Maximum average mail volume for top recipient domains	Set the maximum value that average mail volume can attain before an event is raised. The default is 1000.
Event severity when average mail volume for top recipient domains exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average mail volume for the top *n* recipient domains exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for average mail volume for top recipient domains?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average mail volume for the top *n* recipient domains during the monitoring interval. The default is Yes.
Monitor Sending Domains of Incoming Mail	
Number of top sending domains of incoming mail	Set the top *n* sending domains to be monitored for average mail volume. The default is 10 domains, the minimum is 0, and the maximum is 2147483647. To monitor all domains for average mail volume, enter 0.
Event Notification	
Raise event if average mail volume for top sending domains exceeds threshold?	Select **Yes** to raise an event if the average mail volume for the top *n* sending domains exceeds the threshold you set. The default is Yes.
Threshold - Maximum average mail volume for top sending domains	Set the maximum value that average mail volume can attain before an event is raised. The default is 1000.
Event severity when average mail volume for top sending domains exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average mail volume for the top *n* sending domains exceeds the threshold. The default is 15.
Data Collection	
Collect data for average mail volume for top sending domains?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average mail volume for the top *n* sending domains during the monitoring interval. The default is Yes.
Monitor Senders of Outgoing Mail	
Number of top senders of outgoing mail	Set the top *n* senders of mail to be monitored for average mail volume. The default is 10 senders, the minimum is 0, and the maximum is 2147483647. To monitor all senders for average mail volume, enter 0.
Event Notification	
Raise event if average mail volume for top senders of outgoing mail exceeds threshold?	Select **Yes** to raise an event if the average mail volume for the top *n* senders of mail exceeds the threshold you set. The default is Yes.
Threshold - Maximum average mail volume for top senders of outgoing mail	Set the maximum value that average mail volume can attain before an event is raised. The default is 1000.
Event severity when average mail volume for top senders of outgoing mail exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average mail volume for the top *n* senders of mail exceeds the threshold. The default is 15.
Data Collection	
Collect data for average mail volume for top senders of outgoing mail?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average mail volume for the top *n* senders of mail during the monitoring interval. The default is Yes.
Monitor Recipients of Incoming Mail	
Number of top recipients of incoming mail	Set the top *n* recipients of mail to be monitored for average mail volume. The default is 10 recipients, the minimum is 0, and the maximum is 2147483647. To monitor all recipients for average mail volume, enter 0.
Event Notification	

Parameter	How to Set It
Raise event if average mail volume for top recipients of incoming mail exceeds threshold?	Select **Yes** to raise an event if the average mail volume for the top *n* recipients of mail exceeds the threshold you set. The default is Yes.
Threshold - Maximum average mail volume for top recipients of incoming mail	Set the maximum value that average mail volume can attain before an event is raised. The default is 1000.
Event severity when average mail volume for top recipients of incoming mail exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average mail volume for the top *n* recipients of mail exceeds the threshold. The default is 15.
Data Collection	
Collect data for average mail volume for top recipients of incoming mail?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average mail volume for the top *n* recipients of mail during the monitoring interval. The default is Yes.

ETS_MessageHygiene

Use this Knowledge Script to monitor Edge Transport server message hygiene functions: whether the anti-spam update service is running, the total number of messages that have been filtered as spam, and the number of messages that have been filtered as spam from any one user. You determine which content filter to monitor.

Resource Objects

- Exchange2007_EdgeTransportServer
- Exchange2010_EdgeTransportServer

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ETS_MessageHygiene job fails. The default is 5.
Monitor Anti-Spam Update Service	
Event Notification	
Raise event if anti-spam update service is not running?	Select **Yes** to raise an event if the anti-spam update service is not running. The default is Yes. The anti-spam update service provides daily updates to your content filter.
Event severity when anti-spam update service is not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which the anti-spam update service is not running. The default is 15.
Start anti-spam update service if not running?	Select **Yes** to start the anti-spam update service if it is not running.The default is Yes.
Threshold - Timeout for anti-spam update service to start	Set the number of seconds that AppManager should wait for the anti-spam update service to start before raising an event. The default is 60 seconds.
Raise event if anti-spam update service fails to start?	Select **Yes** to raise an event if AppManager cannot start the anti-spam update service. The default is Yes.
Event severity when anti-spam update service fail to start	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot start the anti-spam service. The default is 5.
Monitor Total Messages Filtered	

Parameter	How to Set It
Include only those messages filtered for these reasons	Provide a comma-separated list of the names of the content filters whose activity you want to monitor. The names do not need to be case-sensitive. One of the many fields in a message is a field titled “Reason.” The content of the Reason field is the filter name you provide in this parameter. Possible filter names are `SCLAtORAboveDeleteThreshold`, `ACLAtOrAboveRejectThreshold`, `BlockListProvide`, and `LocalBlockList`. To monitor all messages, leave this parameter blank. **Note** Quotation marks (“) are not supported in this field. This script returns an error if you enter quotation marks as part of a content filter name.
Event Notification	
Raise event if number of filtered messages exceeds threshold?	Select **Yes** to raise an event if the number of filtered messages from all users exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of filtered messages	Set the maximum number of messages that can be filtered for the reason you specified in *Include only those messages filtered for these reasons*. AppManager raises an event if the number of messages exceeds the threshold. The default is 1000.
Event severity when number of filtered messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of filtered messages exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of filtered messages?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages filtered for the reason you specified in *Include only those messages filtered for these reasons*. The default is No.
Monitor Worst Offenders	
Include only those messages filtered for these reasons	Provide a comma-separated list of the names of the content filters whose activity you want to monitor. The names in the list do not need to be case-sensitive. One of the many fields in a message is a field titled “Reason.” The content of the Reason field is the filter name you provide in this parameter. To monitor all messages, leave this parameter blank. **Note** Quotation marks (“) are not supported in this field. This script returns an error if you enter quotation marks as part of a content filter name.
Maximum number of worst offenders to display	Set the maximum number of worst-offending users to include in an event. These offenders will have sent e-mail that has been filtered as spam for the reasons you indicated in *Include only those messages filtered for these reasons*. The default is 10.
Event Notification	
Raise event if number of filtered messages received from a user exceeds threshold?	Select **Yes** to raise an event if the number of filtered messages from any one user exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of filtered messages received from a user	Set the maximum number of messages that can be filtered for the reason you specified in *Include only those messages filtered for this reason*. AppManager raises an event if the number of messages from one user exceeds the threshold. The default is 100.
Event severity when number of filtered messages received from a user exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of filtered messages from any one user exceeds the threshold. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for number of filtered messages received from worst offenders?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of filtered messages that fit the following criteria: • The messages were filtered for the reasons you specified in *Include only those messages filtered for these reasons*. • The messages were sent from the top *n* worst offending senders. You determine the value of *n* in *Maximum* n*umber of worst offenders to display.* The default is No.

HTS_Connectivity

Use this Knowledge Script to monitor the status of send, receive, and foreign connectors, to monitor connectivity with a Mailbox server, and to monitor the time of the last synchronization with the Edge Transport server. This script raises an event if a threshold is exceeded.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Resource Objects

- Exchange2007_HubTransportServer
- Exchange2010_HubTransportServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Communicate only with Exchange Servers in the local domain?	Select **Yes** to test only Exchange Servers in the same domain as the server on which you run the HTS_Connectivity job. When this option is unselected, the tests attempt to contact *all* Mailbox servers in your organization. These tests will fail if the Exchange accounts in one domain do not have access to other domains.
Ignore these Mailbox servers when testing HTS to MBS communications	Provide a comma-separated list of the hostnames of the Mailbox servers that you want to exclude from availability testing between the Hub Transport server and the Mailbox server.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the HTS_Connectivity job fails. The default is 5.
Monitor Send, Receive, and Foreign Connectors	
Raise event if a send, receive, or foreign connector is disabled?	Select **Yes** to raise an event if a send, receive, or foreign connector is disabled. The default is Yes. The receive connectors receive e-mail from an Edge Transport server, a Mailbox server, or from the Internet when an Edge role is not set up in the Exchange environment. The send connectors send e-mail to the mailbox of the intended recipient or to the Edge Transport server for delivery to another domain. The foreign connectors move e-mail to a server within the organization that does not communicate using SMTP.
Event severity when a connector is disabled	Set the severity level, from 1 to 40, to indicate the importance of an event in which a send, receive, or foreign connector is disabled. The default is 5.

Parameter	How to Set It
Raise event if an enabled receive connector cannot respond to SMTP requests?	Select **Yes** to raise an event if a receive connector is unable to respond to SMTP requests. The default is Yes.
Event severity when a receive connector cannot respond to SMTP requests	Set the severity level, from 1 to 40, to indicate the importance of an event in which a receive connector is unable to respond to SMTP requests. The default is 5.
Monitor Mailbox Server Communication	
Event Notification	
Raise event if unable to communicate with a Mailbox server?	Select **Yes** to raise an event when the Hub Transport server cannot communicate with a Mailbox database on the Mailbox server. The default is Yes. The Hub Transport server transports e-mail to and from the Mailbox server. Therefore, ensuring uninterrupted communication is vital to the health of your Exchange Server 2007 and 2010 environment.
Threshold - Maximum number of seconds to wait before timing out	Set the maximum length of time the Hub Transport server should attempt to contact the Mailbox server before timing out and raising an event. The default is 15 seconds.
Event severity when unable to communicate with a Mailbox server	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Hub Transport server cannot communicate with a Mailbox database on the Mailbox server. The default is 5.
Monitor Edge Synchronization	
Event Notification	
Raise event if this Hub Transport server is not subscribed to any Edge Transport servers?	Select **Yes** to raise an event if the Hub Transport server you are monitoring is not subscribed to an Edge Transport server. AppManager cannot monitor synchronization if the Hub Transport server is not subscribed to the Edge Transport server. Disable this parameter if you will not monitor synchronization with the Edge Transport server. Subscription to the Edge Transport server is not required for AppManager to monitor Mailbox server communication or connector availability. The default is Yes.
Event severity when this Hub Transport server is not subscribed to any Edge Transport servers	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Hub Transport server is not subscribed to an Edge Transport server. The default is 15.
Raise event if time of last Edge synchronization exceeds threshold?	Select **Yes** to raise an event if synchronization between the Edge Transport server and the Hub Transport server has not occurred within the last *n* minutes. The default is Yes. Use the *Threshold - Maximum number of minutes since last Edge synchronization* parameter to determine the value of *n*.
Threshold - Maximum number of minutes since last Edge synchronization	Set the maximum number of minutes that can elapse since the last synchronization before an event is raised. The default is 30 minutes.
Event severity when time of last Edge synchronization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of minutes since the last synchronization exceeds the threshold you set. The default is 15.

HTS_SendersAndRecipients

Use this Knowledge Script to measure average and individual e-mail volume for senders and recipients. This script raises an event if the number of messages or the total size in MB of all messages exceeds the threshold you set.

Resource Objects

- Exchange2007_HubTransportServer
- Exchange2010_HubTransportServer

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Measure mail volume by message count or total message size	Select how this script measures the volume of mail sent to and from your Exchange environment. Choose from **Message count** or **Total message size**. Total message size is measured in MB. The default is Message count.
Comma-separated list of senders and recipients to ignore	Provide a list of e-mail addresses that this script should ignore when measuring e-mail volume. Separate multiple addresses with a comma.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the HTS_SendersAndRecipients job fails. The default is 5.
Monitor Recipients of Internal Mail	
Monitor Average Mail Volume for Recipients of Internal Mail	
Number of top recipients to monitor for average volume	Set the top *n* e-mail recipients whose average internal mail volume you want to monitor. The default is 10 recipients, the minimum is 0, and the maximum is 2147483647. To monitor all recipients for average volume, enter 0.
Event Notification	
Raise event if average volume for top recipients of internal mail exceeds threshold?	Select **Yes** to raise an event if the average mail volume for the top *n* recipients exceeds the threshold you set. The default is Yes.
Threshold - Maximum average volume for top recipients of internal mail	Set the maximum value that average mail volume can attain before an event is raised. The default is 250. Use the *Measure mail volume by message count or total message size* parameter to indicate whether the threshold is in number of messages or Megabytes of message.
Event severity when average volume for top recipients of internal mail exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which average mail volume for the top *n* recipients exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for average volume of top recipients of internal mail?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average mail volume for the top *n* recipients during the monitoring interval. The default is Yes.
Monitor Individual Mail Volume for Recipients of Internal Mail	
Number of top recipients to monitor for individual volume	Set the top *n* e-mail recipients whose individual internal mail volume you want to monitor. The default is 10 recipients, the minimum is 0, and the maximum is 2147483647. To monitor all recipients for individual volume, enter 0.
Event Notification	
Raise event if mail volume for top individual recipients exceeds threshold?	Select **Yes** to raise an event if the individual mail volume for the top *n* recipients exceeds the threshold you set. The default is Yes.
Threshold - Maximum mail volume for individual recipients	Set the maximum value that individual mail volume can attain before an event is raised. The default is 250. Use the *Measure mail volume by message count or total message size* parameter to indicate whether the threshold is in number of messages or Megabytes of message.
Event severity when mail volume for individual recipients exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which individual mail volume for the top *n* recipients exceeds the threshold. The default is 15.
Data Collection	
Collect data for mail volume for individual recipients?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the individual mail volume for the top *n* recipients during the monitoring interval. The default is No.
Monitor Senders of Internal Mail	
Monitor Average Mail Volume for Senders of Internal Mail	
Number of top senders to monitor for average volume	Set the top *n* e-mail senders whose average internal mail volume you want to monitor. The default is 10 senders, the minimum is 0, and the maximum is 2147483647. To monitor all senders for average volume, enter 0.
Event Notification	
Raise event if average volume for top senders of internal mail exceeds threshold?	Select **Yes** to raise an event if the average mail volume for the top *n* senders exceeds the threshold you set. The default is Yes.
Threshold - Maximum average volume for top senders of internal mail	Set the maximum value that average mail volume can attain before an event is raised. The default is 50. Use the *Measure mail volume by message count or total message size* parameter to indicate whether the threshold is in number of messages or Megabytes of message.
Event severity when average volume for top senders of internal mail exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which average mail volume for the top *n* senders exceeds the threshold. The default is 15.
Data Collection	
Collect data for average volume of top senders of internal mail?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average mail volume for the top *n* senders during the monitoring interval. The default is Yes.
Monitor Individual Mail Volume for Senders of Internal Mail	

Parameter	How to Set It
Number of top senders to monitor for individual volume	Set the top *n* e-mail senders whose individual internal mail volume you want to monitor. The default is 10 senders, the minimum is 0, and the maximum is 2147483647. To monitor all senders for individual volume, enter 0.
Event Notification	
Raise event if mail volume for top individual senders exceeds threshold?	Select **Yes** to raise an event if the individual mail volume for the top *n* senders exceeds the threshold you set. The default is Yes.
Threshold - Maximum mail volume for individual senders	Set the maximum value that individual mail volume can attain before an event is raised. The default is 50. Use the *Measure mail volume by message count or total message size* parameter to indicate whether the threshold is in number of messages or Megabytes of message.
Event severity when mail volume for individual senders exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which individual mail volume for the top *n* senders exceeds the threshold. The default is 15.
Data Collection	
Collect data for mail volume for individual senders?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the individual mail volume for the top *n* senders during the monitoring interval. The default is No.

HTS_TransportDumpster

Use this Knowledge Script to monitor Transport Dumpster availability, the number and size of items in the Transport Dumpster, and activity:

- Rate at which items are inserted into the Transport Dumpster
- Rate at which items are deleted from the Transport Dumpster
- Number of items redelivered by the Transport Dumpster

The Transport Dumpster is a container in which recently delivered e-mail is stored. It allows the Hub Transport server to defer the deletion of e-mail so that it can redeliver e-mail after an unscheduled outage.

Resource Objects

- Exchange2007_HubTransportServer
- Exchange2010_HubTransportServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the HTS_TransportDumpster job fails. The default is 5.
Monitor Transport Dumpster Availability	
Event Notification	
Raise event if Transport Dumpster is unavailable?	Select **Yes** to raise an event if the Transport Dumpster cannot be accessed. The default is Yes.
Event severity when Transport Dumpster is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Transport Dumpster cannot be accessed. The default is 5.
Monitor Size of Transport Dumpster	
Data Collection	
Collect data for number of items in Transport Dumpster?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of e-mail messages in the Transport Dumpster during the monitoring interval. The default is No.
Collect data for total size of items currently in Transport Dumpster?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the size of all e-mail messages in MB in the Transport Dumpster during the monitoring interval. The default is No.
Monitor Transport Dumpster Activity	
Data Collection	

Parameter	How to Set It
Collect data for item insertion rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate at which e-mail messages were inserted in the Transport Dumpster during the monitoring interval. The default is No.
Collect data for item deletion rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate at which e-mail messages were deleted from the Transport Dumpster during the monitoring interval. The default is No.
Collect data for item redelivery count?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate at which e-mail messages were redelivered from the Transport Dumpster during the monitoring interval. The default is No.

MBS_ClusterOwner

Use this Knowledge Script to determine whether an Exchange Server is the owner of a node. This script raises an event if the selected server is not the node owner and if the selected Clustered Mailbox Server (CMS) is down.

Note
This script only runs on servers with Exchange Server 2007.

Resource Object

Exchange2007_MailboxServer

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_ClusterOwner job fails. The default is 5.
Monitor Node Ownership	
Raise event if not node owner?	Select **Yes** to raise an event if the selected Exchange Server is not the owner of its node. The default is No.
Event severity when not node owner	Set the severity level, from 1 to 40, to indicate the importance of an event in which the selected Exchange Server is not the owner of the node. The default is 20.
Data Collection	
Collect data for ownership status?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns “0” when the server is not the node owner and “100” if the server is the node owner. The default is Yes.
Monitor Node State	
Event Notification	
Raise event when node is down?	Select **Yes** to raise an event if the node in which the Exchange Server resides is down. The default is Yes.
Event severity when node is down	Set the severity level, from 1 to 40, to indicate the importance of an event in which the node in which the Exchange Server resides is down. The default is 5.
Raise event if CMS is down?	Select **Yes** to raise an event if the Clustered Mailbox Server (CMS) on which the Exchange Server resides is down. The default is Yes.
Event severity when CMS is down	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CMS on which the Exchange Server resides is down. The default is 5.

MBS_DatabaseStateChange

Use this Knowledge Script to monitor changes in the database state, such as active, passive, or suspended, of the mailbox databases on an Exchange Server in a database availability group (DAG) or an Exchange Virtual Server (EVS). This script raises an event if a database is in a specified state, or moves into a specified state.

A job executed on a database in an Exchange Server 2010 DAG causes the job to run on all servers in the DAG. However, only the server that currently owns the database monitors that database.

Note
Exchange Server 2010 does not use storage groups.

Resource Objects

- Exchange2007_MailboxServer
- Exchange2007_Store_Database
- Exchange2007_Store_PFDatabase
- Exchange2010_MailboxServer
- Exchange2010_Store_Database
- Exchange2010_Store_PFDatabase
- Exchange2010_DAG_Databases

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_DatabaseStateChange job fails. The default is 5.
Monitor Database Mount State	
Event Notification	
Raise event if database is unmounted?	Select **Yes** to raise an event if a database is unmounted. When a database is unmounted, the Exchange Server cannot store information in it or read information from it. The default is Yes.
Raise event only when database first becomes unmounted?	Select **Yes** to raise an event only when the database first becomes unmounted. The default is Yes.
Event severity when database is or becomes unmounted	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database is or becomes unmounted. The default is 5.
Automatically mount database if it is currently unmounted?	Select **Yes** to automatically mount a database that is currently unmounted. The default is No.

Parameter	How to Set It
Raise event if database is successfully remounted?	Select **Yes** to raise an event when the database has been successfully remounted. The default is No.
Event severity when database is successfully remounted	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database has been successfully remounted. The default is 25.
Raise event if database fails to mount?	Select **Yes** to raise an event if the database you want to automatically mount fails to mount. The default is no.
Event severity when database fails to mount	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database you want to automatically mount fails to mount. The default is 5.
Monitor Database Copy State	
Event Notification	
Raise event if database copy is suspended?	Select **Yes** to raise an event if the process of copying a database is suspended. The default is Yes.
Raise event only when database first becomes suspended?	Select **Yes** to raise an event only when the database first becomes suspended. The default is Yes.
Event severity when database is or becomes suspended	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database is or becomes suspended. The default is 15.
Raise event if database copy is removed from server?	Select **Yes** to raise an event if a copy of the database is removed. The default is Yes.
Event severity when database copy is removed from the server.	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database is removed from the server. The default is 15.
Monitor Database Active/Passive State	
Event Notification - Database Instances	
Raise event if database is passive?	Select **Yes** to raise an event if a database is passive. The default is Yes.
Raise event only when database first becomes passive?	Select **Yes** to raise an event only when the database first becomes passive. The default is Yes.
Event severity when database is or becomes passive	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database is or becomes passive. The default is 25.
Raise event if database is active?	Select **Yes** to raise an event if a database is active. The default is Yes.
Raise event only when database first becomes active?	Select **Yes** to raise an event only when the database first becomes active. The default is Yes.
Event severity when database is or becomes active	Set the severity level, from 1 to 40, to indicate the importance of an event in which the database is or becomes active. The default is 25.
Event Notification - Database Collection	
Raise event if more than N databases are active?	Select **Yes** to raise an event if more than the specified number of databases are active. The default is Yes.
Raise event only when more than N databases become active?	Select **Yes** to raise an event only when more than the specified number of databases become active. The default is Yes.
Event severity when more than N databases are or become active	Set the severity level, from 1 to 40, to indicate the importance of an event in which more than the specified number of databases are or become active. The default is 15.
Threshold - Maximum number of active databases	Set the highest number of databases that can be active before an event is raised. The default is 3.

Parameter	How to Set It
Raise event if less than N databases are active?	Select **Yes** to raise an event if less than the specified number of databases are active. The default is Yes.
Raise event only when less than N databases become active?	Select **Yes** to raise an event only when less than the specified number of databases become active. The default is Yes.
Event severity when less than N databases are or become active	Set the severity level, from 1 to 40, to indicate the importance of an event in which less than the specified number of databases are or become active. The default is 15.
Threshold - Minimum number of active databases	Set the lowest number of databases that can be active before an event is raised. The default is 1.

MBS_DatabaseStatus

Use this Knowledge Script to monitor mailbox databases for the size of online maintenance window, defragmentation time, free log space, free file space, and number of mailboxes. This script raises an event if a monitored value exceeds or falls below the threshold you set. In addition, this script generates data streams for number of mailboxes in a mailbox database and number of mailboxes in a storage group.

A job executed on a database in an Exchange Server 2010 DAG causes the job to run on all servers in the DAG. However, only the server that currently owns the database monitors that database.

Note
Exchange Server 2010 does not use storage groups.

Resource Objects

- Exchange2007_Store_Group
- Exchange2007_Store_Database
- Exchange2007_MailboxServer
- Exchange2007_Store_PFDatabase
- Exchange2010_MailboxServer
- Exchange2010_DAG_Databases

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_DatabaseStatus job fails. The default is 5.
Monitor Database Defragmentation	
Monitor Size of Online Maintenance Window	
Event Notification	

Parameter	How to Set It
Raise event if online maintenance window is too small or too large?	Select **Yes** to raise an event if online defragmentation occurs too often or not often enough. The default is Yes. You want to ensure that defragmentation of Exchange database occurs often enough, but not too often. Microsoft recommends every 14 days. If you find that defragmentation takes less time, you can shorten your maintenance window. This script compares the values of two Performance Counters to determine whether the size of the maintenance window should be changed: • Online Defrag Pages Freed/Sec • Online Defrag Pages Read/Sec If the read-to-freed ratio is greater than 100:1, then this script raises an event indicating that the size of the maintenance window is too large and should be reduced. If the read-to-freed ratio is less than 50:1, then this script raises an event indicating that the size of the maintenance window is too small and should be increased.
Event severity when online maintenance window is too small or too large	Set the severity level, from 1 to 40, to indicate the importance of an event in which the maintenance window is too small or too large. The default is 15.
Monitor Defragmentation Time	
Event Notification	
Raise event if time to defragment database exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to defragment a database exceeds the threshold you set. The default is Yes.
Threshold - Maximum database defragmentation time	Set the maximum length of time allowed for defragmentation before an event is raised. The default is 10 hours.
Event severity when time to defragment database exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time it takes to defragment a database exceeds the threshold. The default is 15.
Monitor Disk Space	
Event Notification	
Raise event if free space for database files falls below threshold?	Select **Yes** to raise an event if the amount of disk space available for database files falls below the threshold you set. The default is Yes.
Threshold - Minimum free disk space for database files	Set the minimum amount of disk space that must be available for database files to prevent an event from being raised. The default is 1024 MB.
Event severity when free disk space for database files falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the amount of disk space available for database files falls below the threshold. The default is 5.
Raise event if free space for log files falls below threshold?	Select **Yes** to raise an event if the amount of disk space available for log files falls below the threshold you set. The default is Yes.
Threshold - Minimum free disk space for log files	Set the minimum amount of disk space that must be available for log files to prevent an event from being raised. The default is 1024 MB.
Event severity when free disk space for log files falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the amount of disk space available for log files falls below the threshold. The default is 5.
Monitor Mailbox Count	
Monitor Number of Mailboxes Per Storage Group (Exchange 2007 only)	

Parameter	How to Set It
Event Notification	
Raise event if number of mailboxes in a storage group exceeds threshold?	Select **Yes** to raise an event if the number of mailboxes in a storage group exceeds the threshold you set. The default is Yes. A storage group is a logical container only for Exchange Server 2007 databases and their associated system and transaction log files. Exchange Server 2010 does not use storage groups.
Threshold - Maximum number of mailboxes in a storage group	Set the maximum number of mailboxes that can be in a storage group before an event is raised. The default is 2500 mailboxes.
Event severity when number of mailboxes in a storage group exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of mailboxes in a storage group exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of mailboxes in each storage group?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of mailboxes in a storage group during the monitoring period. The default is No.
Monitor Number of Mailboxes Per Mailbox Database	
Event Notification	
Raise event if number of mailboxes in a mailbox database exceeds threshold?	Select **Yes** to raise an event if the number of mailboxes in a database exceeds the threshold you set. The default is Yes. A database stores data, data definitions, indexes, checksums, flags, and other information associated with user mailboxes or public folders.
Threshold - Maximum number of mailboxes in a mailbox database	Set the maximum number of mailboxes that can be in a database before an event is raised. The default is 1000 mailboxes.
Event severity when number of mailboxes in a mailbox database exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of mailboxes in a database exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of mailboxes in each mailbox database?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of mailboxes in a database during the monitoring period. The default is No.
Monitor Disk Activity and Usage	
Data Collection	
Collect data for percentage of elapsed time that the disk was busy servicing read and write requests?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of time that was spent servicing disk reads and disk writes during the monitoring period. The default is No.
Collect data for percentage of elapsed time that the disk was busy servicing read requests?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of time that was spent servicing disk reads during the monitoring period. The default is No.
Collect data for percentage of elapsed time that the disk was busy servicing write requests?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of time that was spent servicing disk writes during the monitoring period. The default is No.
Collect data for average number of both read and write requests that were queued for the disk during the sample interval?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of read and write requests queued for servicing during the monitoring period. The default is No.

MBS_MailboxAccessibility

Use this Knowledge Script to monitor whether the Mailbox server can access specified mailboxes. This script raises an event if the time it takes to connect to a mailbox exceeds the threshold you set.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Resource Objects

- Exchange2007_MailboxServer
- Exchange2007_Store_Group
- Exchange2007_Store_Database
- Exchange2010_MailboxServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_MailboxAccessibility job fails. The default is 5.
Monitor Mailbox Accessibility	
Name of mailbox to be accessed	Provide the name of the mailbox or the mailbox's SMTP address. For example, a mailbox name, `symadmin`, or an SMTP address, `symadmin@golden.local`.
Event Notification	
Raise event if the mailbox cannot be accessed?	Select **Yes** to raise an event if the Mailbox server cannot access the specified mailbox. The default is Yes. A mailbox is inaccessible when it does not exist.
Event severity when the mailbox cannot be accessed	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Mailbox server cannot access the specified mailbox. The default is 5.
Raise event if response time for accessing the mailbox exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes to connect to the specified mailbox exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for accessing the mailbox	Set the maximum length of time that the Mailbox server should wait to connect with the specified mailbox before raising an event. The default is 1000 milliseconds. The minimum is 1 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the time it takes to access the specified mailbox exceeds the threshold you set. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for mailbox access response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the response time for mailbox access during the monitoring period. The default is No.

MBS_MailboxUsage

Use this Knowledge Script to measure the size of mailboxes by either the number of messages in the mailbox, or by total message size in MB. You can monitor average mailbox size and individual mailbox size for the top *n* mailboxes. This script raises an event if average mailbox size and individual mailbox size exceed the threshold you set.

A job executed on a database in an Exchange Server 2010 DAG causes the job to run on all servers in the DAG. However, only the server that currently owns the database monitors that database.

Resource Objects

- Exchange2007_MailboxServer
- Exchange2007_Store_Group
- Exchange2007_Store_Database
- Exchange2010_MailboxServer
- Exchange2010_DAG_Databases

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Measure mailbox size in MB or by number of messages	Select how you want to measure the size of mailboxes: • Choose **Message count** to measure the size of mailboxes by the number of messages in the mailboxes • Choose **Total message size** to measure the size of all messages in the mailboxes in MB. The default is Total message size.
Comma-separated list of mailboxes to ignore	Provide a list of mailbox display names that this script should ignore when measuring mailbox size. Separate the names with a comma. **Note** Ensure you provide the mailbox display name, not the mailbox alias.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_MailboxUsage job fails. The default is 5.
Monitor Average Mailbox Size	
Number of largest mailboxes to be averaged	Set the top *n* mailboxes whose average size you want to monitor. The default is 10 mailboxes, the minimum is 0, and the maximum is 2147483647
Event Notification	

Parameter	How to Set It
Raise event if average mailbox size exceeds threshold?	Select **Yes** to raise an event if the average size of the top *n* mailboxes exceeds the threshold you set. The default is Yes. Use the *Number of largest mailboxes to be averaged* parameter to determine the value of *n*. AppManager uses Exchange cmdlets to determine the largest mailboxes, based on number and size of mailboxes and messages.
Threshold -- Maximum average mailbox size in MB or by number of messages	Set the maximum average size that the top *n* mailboxes can attain before an event is raised. The default is 100. The average is based on either the total number of messages in the top *n* mailboxes, or the total size in MB of the top *n* mailboxes, depending on your selection in the *Measure mailbox size by total message size or message count* parameter.
Event severity when average mailbox size exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average size of the top *n* mailboxes exceeds the threshold. The default is 5.
Data Collection	
Collect data for average mailbox size?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns one of the following data streams: • Average number of messages in *n* largest mailboxes • Average size in MB of the *n* largest mailboxes The default is No.
Monitor Individual Mailbox Size	
Number of largest mailboxes to be monitored	Set the top *n* mailboxes whose individual size you want to monitor. The default is 10 mailboxes, the minimum is 0, and the maximum is 2147483647.
Event Notification	
Raise event if individual mailbox size exceeds threshold?	Select **Yes** to raise an event if the size of any one of the top *n* mailboxes exceeds the threshold you set. The default is Yes. Use the *Number of largest mailboxes to be monitored* parameter to determine the value of *n*. AppManager uses Exchange cmdlets to determine the largest mailboxes, based on number and size of mailboxes and messages.
Threshold - Maximum individual mailbox size in MB or by number of messages	Set the maximum size that any one of the top *n* mailboxes can attain before an event is raised. The default is 250. The size is based on either the total number of messages in the top *n* mailboxes, or the total size in MB of the top *n* mailboxes, depending on your selection in the *Measure mailbox size by message count or total message size* parameter.
Event severity when individual mailbox size exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the size of any one of the top *n* mailboxes exceeds the threshold. The default is 5.
Data Collection	
Collect data for individual mailbox size?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the following data streams: • Number of messages in each of the *n* largest mailboxes • Size in MB of each of the *n* largest mailboxes Use the *Number of largest mailboxes to be monitored* parameter to determine the value of *n*. The default is No.

MBS_MailFlow

Use this Knowledge Script to test the flow of mail by sending test e-mail to local or remote Mailbox servers. This script raises an event if the test fails or if response time exceeds the threshold you set.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Resource Objects

- Exchange2007_MailboxServer
- Exchange2010_MailboxServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_MailFlow job fails. The default is 5.
Monitor Mail Flow	
Comma-separated list of target Mailbox servers	Provide the hostnames or IP addresses of the Mailbox servers to which you want to send test e-mail. Separate the names or addresses with a comma.
Comma-separated list of recipient e-mail addresses	Provide the e-mail addresses to which you want to send test e-mail. Separate the addresses with a comma.
Event Notification	
Raise event if mail flow test fails?	Select **Yes** to raise an event if test mail cannot be sent to the selected Mailbox servers. The default is Yes.
Event severity when mail flow test fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which test mail cannot be sent to the selected Mailbox servers. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the elapsed time to send mail to the Mailbox servers exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time for mail flow test	Set the maximum number of milliseconds that can elapse while sending mail to the selected Mailbox servers before an event is raised. The default is 10,000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which response time exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for mail flow response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the response time for the mail flow tests during the monitoring period. The default is No.

MBS_MessagingRecordsMgmt

Use this Knowledge Script to monitor Messaging Records Management (MRM) tasks such as deleting, journaling, moving, and retention, and to monitor the Windows Event log for MRM-related events. This script raises an event if a threshold is exceeded.

Resource Objects

- Exchange2007_MailboxServer
- Exchange2010_MailboxServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_MessagingRecordsManagement job fails. The default is 5.
Monitor Messaging Records Management	
Monitor Messages Deleted But Recoverable	
Event Notification	
Raise event if number of messages deleted but recoverable exceeds threshold?	Select **Yes** to raise an event if the number of deleted, but recoverable, messages exceeds the threshold you set. The default is Yes. Exchange can recover messages that users have deleted from their Deleted Items folders. You can use Exchange System Manager to define how many days a deleted message stays in the mailbox store before being permanently deleted.
Event severity when number of messages deleted but recoverable exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of recoverable messages exceeds the threshold you set. The default is 15.
Threshold - Maximum number of messages deleted but recoverable	Set the maximum number of recoverable messages that can be in the mailbox store before an event is raised. The default is 1000 messages.
Data Collection	
Collect data for number of messages deleted but recoverable?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of recoverable messages deleted during the monitoring interval. The default is Yes.
Monitor Messages Permanently Deleted	
Event Notification	

Parameter	How to Set It
Raise event if number of messages permanently deleted exceeds threshold?	Select **Yes** to raise an event if the number of permanently deleted messages exceeds the threshold you set. The default is Yes. You can use Exchange System Manager to define how many days a deleted message stays in the mailbox store before being permanently deleted.
Event severity when number of messages permanently deleted exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of permanently deleted messages exceeds the threshold you set. The default is 15.
Threshold - Maximum number of messages permanently deleted	Set the maximum number of messages that can be permanently deleted before an event is raised. The default is 1000 messages.
Data Collection	
Collect data for number of messages permanently deleted?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages permanently deleted during the monitoring interval. The default is Yes.
Monitor Messages Journaled	
Event Notification	
Raise event if number of messages journaled exceeds threshold?	Select **Yes** to raise an event if the number of journaled, or archived, messages exceeds the threshold you set. The default is Yes. The Exchange Journaling feature allows users to archive all incoming and outgoing e-mail for a specific mailbox store.
Event severity when number of messages journaled exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of archived messages exceeds the threshold you set. The default is 15.
Threshold - Maximum number of messages journaled	Set the maximum number of messages that can be archived before an event is raised. The default is 1000 messages.
Data Collection	
Collect data for number of messages journaled?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages journaled during the monitoring interval. The default is Yes.
Monitor Messages Moved	
Event Notification	
Raise event if number of messages moved exceeds threshold?	Select **Yes** to raise an event if the number of messages moved from one managed folder to another exceeds the threshold you set. The default is Yes.
Event severity when number of messages moved exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of moved messages exceeds the threshold you set. The default is 15.
Threshold - Maximum number of messages moved	Set the maximum number of messages that can be moved before an event is raised. The default is 1000 messages.
Data Collection	
Collect data for number of messages moved?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages moved during the monitoring interval. The default is Yes.
Monitor Messages Past Retention	
Event Notification	

Parameter	How to Set It
Raise event if number of messages marked as past retention date exceeds threshold?	Select **Yes** to raise an event if the number of deleted messages that have passed their retention date exceeds the threshold you set. The default is Yes. Use Exchange System Manager to define how many days a deleted message stays in the mailbox store.
Event severity when number of messages marked as past retention date exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of expired messages exceeds the threshold you set. The default is 15.
Threshold - Maximum number of messages marked as past retention date	Set the maximum number of messages that can have passed their retention date before an event is raised. The default is 1000 messages.
Data Collection	
Collect data for number of messages marked as past retention date?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages that expired during the monitoring interval. The default is Yes.
Monitor Windows Event Log for Messaging Records Management Events	
Event Notification	
Comma-separated list of event sources to ignore	Provide a list of event sources that this script should ignore when scanning the Windows Event log. Separate the source names with a comma. Event sources are computers whose names are displayed in the Source column of the event log.
Comma-separated list of event categories to ignore	Provide a list of event categories that this script should ignore when scanning the Windows Event log. Separate the category names with a comma.
Comma-separated list of event IDs to ignore	Provide a list of error and warning ID numbers that this script should ignore when scanning the Windows Event log. Separate the numbers with a comma.
Raise event if MRM error events are found?	Select **Yes** to raise an event if MRM error events are found in the Windows Event Log. The default is Yes.
Event severity when MRM error events are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Windows Event Log contains MRM error events. The default is 10.
Raise event if MRM warning events are found?	Select **Yes** to raise an event if MRM warning events are found in the Windows Event Log. The default is Yes.
Event severity when MRM warning events are found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Windows Event Log contains MRM warning events. The default is 20.

MBS_PublicFolderUsage

Use this Knowledge Script to measure the size of public folders by the number of messages in the folders or by total message size in MB. You can monitor average folder size and individual folder size for the top *n* folders. This script raises an event if average folder size and individual folder size exceed the threshold you set.

Resource Objects

- Exchange2007_Store_Group
- Exchange2007_Store_PFDatabase
- Exchange2010_Store_PFDatabase

Default Schedule

By default, this script runs every one hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Measure public folder size by message count or total message size	Select how you want to measure the size of public folders: • Choose **Message count** to measure the size of folders by the number of messages in the mailboxes. • Choose **Total message size** to measure the size of all messages in the folders in MB. The default is Total message size.
Comma-separated list of public folders to ignore	Provide a list of public folder names that this script should ignore when measuring folder size. Separate the names with a comma.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_PublicFolderUsage job fails. The default is 5.
Monitor Average Public Folder Size	
Number of largest public folders to be averaged	Set the top *n* public folders whose average size you want to monitor. The default is 10 folders.
Event Notification	
Raise event if average public folder size exceeds threshold?	Select **Yes** to raise an event if the average size of the top *n* public folders exceeds the threshold you set. The default is Yes. Use the *Number of largest public folders to be averaged* parameter to determine the value of *n*. AppManager uses Exchange cmdlets to determine the largest public folders, based on number and size of folders and messages.

Parameter	How to Set It
Threshold - Maximum average public folder size	Set the maximum average size that the top *n* public folders can attain before an event is raised. The default is 25. The average is based on either the total number of messages in the top *n* folders, or the total size in MB of the top *n* folders, depending on your selection in the *Measure public folder size by message count or total message size* parameter.
Event severity when average public folder size exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average size of the top *n* public folders exceeds the threshold. The default is 5.
Data Collection	
Collect data for average public folder size?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns one of the following data streams: • Average number of messages in *n* largest public folders • Average size (MB) of the *n* largest public folders The default is No.
Monitor Individual Public Folder Size	
Number of largest public folders to be monitored	Set the top *n* public folders whose individual size you want to monitor. The default is 10 folders.
Event Notification	
Raise event if individual public folder size exceeds threshold?	Select **Yes** to raise an event if the size of any one of the top *n* public folders exceeds the threshold you set. The default is Yes. Use the *Number of largest public folders to be monitored* parameter to determine the value of *n*. AppManager uses Exchange cmdlets to determine the largest public folders, based on number and size of folders and messages.
Threshold - Maximum individual public folder size	Set the maximum size that any one of the top *n* public folders can attain before an event is raised. The default is 100. The size is based on either the total number of messages in the top *n* public folders, or the total size in MB of the top *n* public folders, depending on your selection in the *Measure public folder size by message count or total message size* parameter.
Event severity when individual public folder size exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the size of any one of the top *n* public folders exceeds the threshold. The default is 5.
Data Collection	
Collect data for individual public folder size?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the following data streams: • Number of messages in each of the *n* largest public folders • Size (MB) of each of the *n* largest public folders Use the *Number of largest public folders to be monitored* parameter to determine the value of *n*. The default is No.

MBS_Replication

Use this Knowledge Script to monitor replication status and performance for a Mailbox server. This script raises an event when a threshold is exceeded and generates data streams for the following metrics:

- Replication latency
- Number of pending replication transactions
- Replication rate
- Number of replications in the copy and replay queues

This script also monitors the availability of the File Share Witness, a requirement for using the cluster continuous replication (CCR) functionality in Exchange Server 2007. CCR enables the continuous and asynchronous updating of a second copy of a database with the changes that have been made to the active copy of the database. The File Share Witness is a file share that is external to a cluster and helps determine the status of the cluster.

Prerequisite

The AppManager agent (`netiqmc` service) must have permission to access the File Share Witness folder to collect data for File Share Witness usage on a two-node CCR cluster.

Resource Objects

- Exchange2007_MailboxServer
- Exchange2010_MailboxServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Communicate only with Exchange servers in the local domain?	Select **Yes** to test only Exchange servers in the same domain as the server on which you run the MBS_Replication job. The default is No. When this option is unselected, the job attempts to contact *all* Exchange Servers in your organization. These attempts will fail if the Exchange accounts in one domain do not have access to other domains.
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MBS_Replication job fails. The default is 5.
Monitor Replication Agent	
Event Notification	
Raise event if replication agent is not running?	Select **Yes** to raise an event if the replication agent is not running. The default is Yes.

Parameter	How to Set It
Event severity when replication agent is not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which the replication agent is not running. The default is 5.
Start replication agent if not running?	Select **Yes** to start the replication agent if it is not running. The default is Yes.
Threshold - Maximum timeout for starting replication agent	Set the maximum length of time the script can attempt to start the replication agent before timing out and raising an event. The default is 60 seconds.
Raise event if replication agent fails to start?	Select **Yes** to raise an event if the script cannot start the replication agent. The default is Yes.
Event severity when replication agent fails to start	Set the severity level, from 1 to 40, to indicate the importance of an event in which the script cannot start the replication agent. The default is 5.
Monitor Replication Copy Status	
Event Notification	
Raise event if replication is unhealthy?	Select **Yes** to raise an event if replication is unhealthy. The default is Yes. This script uses the `Get-StorageGroupCopyStatus` cmdlet to determine the status, or health, of the replication function. If the status is `Failed` or `Not Supported`, then replication is considered unhealthy. Replication is also considered unhealthy if the number of transactions in the copy queue or the replay queue exceeds the threshold you set.
Threshold - Maximum length of copy queue	Set the maximum number of transactions that can be waiting in the copy queue before an event is raised. The default is 3 transactions.
Threshold - Maximum length of replay queue	Set the maximum number of transactions that can be waiting in the replay queue before an event is raised. The default is 20 transactions.
Event severity when replication is unhealthy	Set the severity level, from 1 to 40, to indicate the importance of an event in which replication is determined to be unhealthy. The default is 5.
Data Collection	
Collect data for copy queue length?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of replication transactions in the copy queue for the monitoring period. The default is No.
Collect data for replay queue length?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of replication transactions in the replay queue for the monitoring period. The default is No.
Monitor File Share Witness	
Raise event if File Share Witness is unavailable?	Select **Yes** to raise an event if the File Share Witness is unavailable. The default is Yes.
Event severity when File Share Witness is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the File Share Witness is unavailable. The default is 15.
Monitor File Share Witness Usage on Two-node CCR Setup	
Data Collection	
Collect data for File Share Witness usage on two-node CCR setup?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of usage for the File Share Witness in a two-node cluster continuous replication environment. The default is No.
Monitor Replication Latency	
Event Notification	

Parameter	How to Set It

Raise event if replication latency exceeds threshold?	Select **Yes** to raise an event if replication latency exceeds the threshold you set. The default is Yes.
	When this parameter is set to **Yes**, the Extended ESE performance counters in the registry are enabled. The following updates are made automatically in the registry values:
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ESE\Performance`
	`Value Name: Show Advanced Counters`
	`Data Type: REG_DWORD`
	`Value: 1`

Threshold -- Maximum replication latency	Set the maximum number of milliseconds allowed for replication latency before an event is raised. The default is 20000 milliseconds.
Event severity when replication latency exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which replication latency exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for replication latency?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the total latency for the monitoring period. The default is No.
Monitor Replication Rate	
Event Notification	
Raise event if replication rate exceeds threshold?	Select **Yes** to raise an event if the replication rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum replication rate	Set the maximum number of replications allowed per minute before an event is raised. The default is 10000 transactions.
Event severity when replication rate threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the replication rate exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for replication rate?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the replication rate for the monitoring period. The default is No.
Monitor Pending Replication Transactions	
Event Notification	
Raise event if pending replication transactions exceed threshold?	Select **Yes** to raise an event if the number of transactions waiting to be replicated exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of pending replication transactions	Set the maximum number of transactions that can be awaiting replication before an event is raised. The default is 500 transactions.
Event severity when pending replication transactions exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of transactions waiting to be replicated exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for pending replication transactions?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of pending replication transactions for the monitoring period. The default is No.

Transport_BackPressure

Use this Knowledge Script to monitor the status of back pressure for the Hub Transport server.

Back pressure monitors system resources, such as available disk space and available memory, on computers that have the Hub Transport server role or Edge Transport server role installed. If resource usage exceeds a certain level, the Exchange server stops accepting new connections and messages, but may continue to deliver existing messages. When resource usage returns to a normal level, the Exchange server accepts new connections and messages.

This script raises events for three levels of resource usage:

- **Normal**. No back pressure is applied to the server: new connections and messages are accepted.
- **Medium**. The resource is slightly overused. Limited back pressure is applied to the server: incoming mail from the authoritative domain is allowed, but new connections and messages from other sources are rejected.
- **High**. The resource is severely overused. Full back pressure is applied to the server: all message flow stops, and all new connections and messages are rejected.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Resource Objects

- Exchange2007_HubTransportServer
- Exchange2007_EdgeTransportServer
- Exchange2010_HubTransportServer
- Exchange2010_EdgeTransportServer

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Transport_BackPressure job fails. The default is 5.
Monitor Back Pressure Status	
Event Notification	
Raise event if back pressure is high?	Select **Yes** to raise an event if resource usage is at a high level. The default is Yes.
Event severity when back pressure is high	Set the severity level, from 1 to 40, to indicate the importance of an event in which resource usage is at a high level. The default is 5.

Parameter	How to Set It
Raise event if back pressure is medium?	Select **Yes** to raise an event if resource usage is at a medium level. The default is Yes.
Event severity when back pressure is medium	Set the severity level, from 1 to 40, to indicate the importance of an event in which resource usage is at a medium level. The default is 10.

Transport_QueueStatus

Use this Knowledge Script to monitor the number of messages in Hub Transport server queues:

- **Submission queue**, which contains messages waiting to be categorized and routed to a delivery queue.
- **Mailbox delivery queue**, which contains messages awaiting delivery to mailboxes on a Mailbox server that is located in the same site as the Hub Transport server.
- **Remote delivery queue**, which contains messages awaiting delivery to mailboxes outside the Active Directory site in which the Hub Transport server is located.
- **Poison message queue**, which is a quarantine destination for messages identified as potentially fatal to your Exchange Server 2007 or 2010 environment.
- **Unreachable destination queue**, which contains messages that cannot be routed to their destinations.

This script raises an event if the length of a queue or the change in the length of a queue exceeds the threshold you set.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Resource Objects

- Exchange2007_Queue
- Exchange2007_EdgeTransportServer
- Exchange2007_HubTransportServer
- Exchange2010_Queue
- Exchange2010_EdgeTransportServer
- Exchange2010_HubTransportServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Transport_QueueStatus job fails. The default is 5.
Monitor Submission Queue	
Event Notification	

Parameter	How to Set It
Raise event if number of queued messages exceeds threshold?	Select **Yes** to raise an event if the number of messages in the submission queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of messages in queue	Set the maximum number of messages that can be waiting in the submission queue before an event is raised. The default is 100 messages.
Event severity when number of messages in queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in the submission queue exceeds the threshold you set. The default is 15.
Raise event if increase in queued messages exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in the number of messages in the submission queue exceeds the threshold. The script measures the rate of increase since the last iteration of the job. The default is No.
Threshold - Maximum percent increase in queued messages since last job iteration	Set the maximum acceptable percentage of increase in queue size since the last job iteration. AppManager raises an event if the percentage of increase exceeds this value. The default is 50%.
Event severity when increase in queued messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in the number of messages in the submission queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of messages in the submission queue?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages in the submission queue during the monitoring interval. The default is No.
Monitor Mailbox Delivery Queue	
Event Notification	
Raise event if number of queued messages exceeds threshold?	Select **Yes** to raise an event if the number of messages in the mailbox delivery queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of messages in queue	Set the maximum number of messages that can be waiting in the mailbox delivery queue before an event is raised. The default is 250 messages.
Event severity when number of messages in queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in the mailbox delivery queue exceeds the threshold you set. The default is 15.
Raise event if increase in queued messages exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in the number of messages in the mailbox delivery queue exceeds the threshold. The script measures the rate of increase since the last iteration of the job. The default is No.
Threshold - Maximum percent increase in queued messages since last job iteration	Set the maximum acceptable percentage of increase in queue size since the last job iteration. AppManager raises an event if the percentage of increase exceeds this value. The default is 50%.
Event severity when increase in queued messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in the number of messages in the mailbox delivery queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of messages in the mailbox delivery queue?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages in the mailbox delivery queue during the monitoring interval. The default is No.
Monitor Remote Delivery Queue	
Event Notification	

Parameter	How to Set It
Raise event if number of queued messages exceeds threshold?	Select **Yes** to raise an event if the number of messages in the remote delivery queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of messages in queue	Set the maximum number of messages that can be waiting in the remote delivery queue before an event is raised. The default is 250 messages.
Event severity when number of messages in queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in the remote delivery queue exceeds the threshold you set. The default is 15.
Raise event if increase in queued messages exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in the number of messages in the remote delivery queue exceeds the threshold. The script measures the rate of increase since the last iteration of the job. The default is No.
Threshold - Maximum percent increase in queued messages since last job iteration	Set the maximum acceptable percentage of increase in queue size since the last job iteration. AppManager raises an event if the percentage of increase exceeds this value. The default is 50%.
Event severity when increase in queued messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in the number of messages in the remote delivery queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of messages in the remote delivery queue?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages in the remote delivery queue during the monitoring interval. The default is No.
Monitor Poison Message Queue	
Event Notification	
Raise event if number of queued messages exceeds threshold?	Select **Yes** to raise an event if the number of messages in the poison message queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of messages in queue	Set the maximum number of messages that can be waiting in the poison message queue before an event is raised. The default is 0 (zero) messages.
Event severity when number of messages in queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in the poison message queue exceeds the threshold you set. The default is 15.
Raise event if increase in queued messages exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in the number of messages in the poison message queue exceeds the threshold. The script measures the rate of increase since the last iteration of the job. The default is No.
Threshold - Maximum percent increase in queued messages since last job iteration	Set the maximum acceptable percentage of increase in queue size since the last job iteration. AppManager raises an event if the percentage of increase exceeds this value. The default is 50%.
Event severity when increase in queued messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in the number of messages in the poison message queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of messages in the poison message queue?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages in the poison message queue during the monitoring interval. The default is No.
Monitor Unreachable Destination Queue	
Event Notification	

Parameter	How to Set It
Raise event if number of queued messages exceeds threshold?	Select **Yes** to raise an event if the number of messages in the unreachable destination queue exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of messages in queue	Set the maximum number of messages that can be waiting in the unreachable destination queue before an event is raised. The default is 100 messages.
Event severity when number of messages in queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in the unreachable destination queue exceeds the threshold you set. The default is 15.
Raise event if increase in queued messages exceeds threshold?	Select **Yes** to raise an event if the percentage of increase in the number of messages in the unreachable destination queue exceeds the threshold. The script measures the rate of increase since the last iteration of the job. The default is No.
Threshold - Maximum percent increase in queued messages since last job iteration	Set the maximum acceptable percentage of increase in queue size since the last job iteration. AppManager raises an event if the percentage of increase exceeds this value. The default is 50%.
Event severity when increase in queued messages exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of increase in the number of messages in the unreachable destination queue exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of messages in the unreachable queue?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages in the unreachable destination queue during the monitoring interval. The default is No.

UMS_CallActivity

Use this Knowledge Script to monitor call activity on a Unified Messaging server. This script raises an event if a threshold is exceeded and generates data streams for the following types of calls:

- Active voice calls
- Active fax calls
- Active play-on-phone calls
- Active auto-attendant calls
- Active subscriber-access calls
- Active prompt-editing calls

Resource Objects

- Exchange2007_UnifiedMessagingServer
- Exchange2010_UnifiedMessagingServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UMS_CallActivity job fails. The default is 5.
Monitor Voice Calls	
Event Notification	
Raise event if number of active voice calls exceeds threshold?	Select **Yes** to raise an event if the number of active voice calls exceeds the threshold you set. The default is Yes. Active voice calls are calls that are currently connected to the Unified Messaging server.
Threshold - Maximum number of active voice calls	Set the maximum number of calls that can be simultaneously connected to the Unified Messaging server before an event is raised. The default is 100 calls.
Event severity when number of active voice calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active voice calls exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of active voice calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of voice calls that were active during the monitoring period. The default is No.
Monitor Fax Calls	

Parameter	How to Set It
Event Notification	
Raise event if number of active fax calls exceeds threshold?	Select **Yes** to raise an event if the number of active fax calls exceeds the threshold you set. The default is Yes. Voice calls become fax calls after a fax tone is detected.
Threshold - Maximum number of active fax calls	Set the maximum number of fax calls that can be simultaneously connected to the Unified Messaging server before an event is raised. The default is 100 calls.
Event severity when number of active fax calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active fax calls exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of active fax calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of fax calls that were active during the monitoring period. The default is No.
Monitor Play On Phone Calls	
Event Notification	
Raise event if number of active play on phone calls exceeds threshold?	Select **Yes** to raise an event if the number of active play-on-phone calls exceeds the threshold you set. The default is Yes. The Exchange Server 2007 Unified Messaging play-on-phone feature enables users to access voice mail messages on the telephone rather than on their computer speakers. Active play-on-phone calls are outbound calls initiated to play back messages.
Threshold - Maximum number of active play on phone calls	Set the maximum number of play-on-phone calls that can be simultaneously active before an event is raised. The default is 100 calls.
Event severity when number of active play on phone calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active play-on-phone calls exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of active play on phone calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of play-on-phone calls that were active during the monitoring period. The default is No.
Monitor Auto Attendant Calls	
Event Notification	
Raise event if number of active auto attendant calls exceeds threshold?	Select **Yes** to raise an event if the number of active auto-attendant calls exceeds the threshold you set. The default is Yes. The Unified Messaging auto attendant is a set of voice prompts or .wav files played to callers in place of a human operator when they call into your organization. Active auto-attendant calls are calls that are currently connected to the Unified Messaging server by the auto attendant.
Threshold - Maximum number of active auto attendant calls	Set the maximum number of auto-attendant calls that can be simultaneously active before an event is raised. The default is 100 calls.
Event severity when number of active auto attendant calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active auto-attendant calls exceeds the threshold. The default is 5.
Data Collection	

Parameter	How to Set It
Collect data for number of active auto attendant calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of auto-attendant calls that were active during the monitoring period. The default is No.
Monitor Subscriber Access Calls	
Event Notification	
Raise event if number of active subscriber access calls exceeds threshold?	Select **Yes** to raise an event if the number of active subscriber-access calls exceeds the threshold you set. The default is Yes. Subscriber access is used by users to access their individual mailboxes to retrieve e-mail, voice messages, contacts, and calendaring information. Active subscriber-access calls are logged-on subscribers who are currently connected to the Unified Messaging server.
Threshold - Maximum number of active subscriber access calls	Set the maximum number of subscriber-access calls that can be simultaneously active before an event is raised. The default is 100 calls.
Event severity when number of active subscriber access calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active subscriber-access calls exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of active subscriber access calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of subscriber-access calls that were active during the monitoring period. The default is No.
Monitor Prompt Editing Calls	
Event Notification	
Raise event if number of active prompt editing calls exceeds threshold?	Select **Yes** to raise an event if the number of active prompt-editing calls exceeds the threshold you set. The default is Yes. Active prompt-editing calls are logged-on users who are editing custom prompts, such as voice-mail greetings.
Threshold - Maximum number of active prompt editing calls	Set the maximum number of prompt-editing calls that can be simultaneously active before an event is raised. The default is 100 calls.
Event severity when number of active prompt editing calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of active prompt-editing calls exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of active prompt editing calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of prompt-editing calls that were active during the monitoring period. The default is No.

UMS_Connectivity

Use this Knowledge Script to monitor connectivity to Hub Transport servers, Mailbox servers, Active Directory, and mailboxes enabled for Unified Messaging (UM). This script raises an event if a connectivity test fails or if response time exceeds the threshold you set.

A mailbox that is enabled for UM can receive e-mail, voicemail, and fax messages.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Resource Objects

- Exchange2007_UnifiedMessagingServer
- Exchange2010_UnifiedMessagingServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UMS_Connectivity job fails. The default is 5.
Monitor UM-Enabled Mailbox Accessibility	
Dial plan to use to connect to the UM-enabled mailbox	Identify the dial plan to use to connect to the mailbox you want to monitor. You may have more than one dial plan in use in your Exchange Server 2007 environment. Separate multiple dial plans with a comma.
Phone extension of UM-enabled mailbox to use for accessibility test	Provide the extension number of the mailbox you want to monitor.
PIN of UM-enabled mailbox to use for accessibility test	Provide the Personal Identification Number (PIN) required to access the mailbox you want to monitor.
Event Notification	
Raise event if UM-enabled mailbox cannot be accessed?	Select **Yes** to raise an event if the specified mailbox cannot be tested for connectivity. The default is Yes.
Event severity when UM-enabled mailbox cannot be accessed	Set the severity level, from 1 to 40, to indicate the importance of an event in which the specified mailbox is unavailable for testing. The default is 5.
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if the time to connect to the mailbox exceeds the threshold you set. The default is Yes.
Threshold - Maximum response time	Set the maximum number of seconds that AppManager should wait to connect with the mailbox before raising an event. The default is 10000 milliseconds.

Parameter	How to Set It
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which response time exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for response time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the length of response time during the monitoring period. The default is No.
Monitor Mailbox Server Connectivity	
Event Notification	
Raise event if Mailbox servers are unavailable?	Select **Yes** to raise an event if Mailbox servers cannot be tested for connectivity. The default is Yes.
Event severity when Mailbox servers are unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Mailbox servers are unavailable for testing. The default is 5.
Monitor Hub Transport Server Connectivity	
Event Notification	
Raise event if Hub Transport servers are unavailable?	Select **Yes** to raise an event if Hub Transport servers cannot be tested for connectivity. The default is Yes.
Event severity when Hub Transport servers are unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Hub Transport servers are unavailable for testing. The default is 5.
Monitor Mailbox Server Connectivity	
Event Notification	
Raise event if Mailbox servers are unavailable?	Select **Yes** to raise an event if Mailbox servers cannot be tested for connectivity. The default is Yes.
Event severity when Mailbox servers are unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Mailbox servers are unavailable for testing. The default is 5.
Monitor Active Directory Connectivity	
Event Notification	
Raise event if Active Directory is unavailable?	Select **Yes** to raise an event if Active Directory cannot be tested for connectivity. The default is Yes.
Event severity when Active Directory is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Active Directory is unavailable for testing. The default is 5.

UMS_Failures

Use this Knowledge Script to monitor failures of the Unified Messaging server related to redirected calls, disconnected calls, and access to Active Directory, the Hub Transport server, and the Mailbox server. This script raises an event if a threshold is exceeded.

This script is a member of the Exchange2007 recommended Knowledge Script Group. For more information, see "Recommended Knowledge Script Group" on page 2026.

Resource Objects

- Exchange2007_UnifiedMessagingServer
- Exchange2010_UnifiedMessagingServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UMS_Failures job fails. The default is 5.
Monitor Calls Disconnected Due to Internal Errors	
Event Notification	
Raise event if calls disconnected due to internal errors exceed threshold?	Select **Yes** to raise an event if the number of calls disconnected due to internal errors exceeds the threshold you set. The default is Yes. This script uses the value of the `Calls Disconnected on Irrecoverable Internal Error` performance counter, which is the number of calls that were disconnected after an internal system error occurred.
Threshold - Maximum number of calls disconnected due to internal errors	Set the maximum number of calls that can be disconnected due to an internal error before an event is raised. The default is 900 calls.
Event severity when calls disconnected due to internal errors exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of calls disconnected due to internal errors exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for calls disconnected due to internal errors	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls disconnected due to internal errors during the monitoring period. The default is No.
Monitor Calls Disconnected Due to External Errors	
Event Notification	

Parameter	How to Set It
Raise event if calls disconnected due to external errors exceed threshold?	Select **Yes** to raise an event if the number of calls disconnected due to external errors exceeds the threshold you set. The default is Yes. This script uses the value of the `Calls Disconnected by UM on Irrecoverable External Error` performance counter, which is the total number of calls that have been disconnected after an irrecoverable external error occurred.
Threshold - Maximum number of calls disconnected due to external errors	Set the maximum number of calls that can be disconnected due to an external error before an event is raised. The default is 900 calls.
Event severity when calls disconnected due to external errors exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of calls disconnected due to external errors exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for calls disconnected due to external errors?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls disconnected due to external errors during the monitoring period. The default is No.
Monitor Failures to Redirect Calls	
Event Notification	
Raise event if failures to redirect calls exceed threshold?	Select **Yes** to raise an event if the number of failed attempts to redirect calls exceeds the threshold you set. The default is Yes. This script uses the value of the `Failed to Redirect Call` performance counter, which is the number of times the Unified Messaging service did not redirect calls to a Unified Messaging worker process.
Threshold - Maximum number of failures to redirect calls	Set the maximum number of calls that can fail to be redirected before an event is raised. The default is 900 calls.
Event severity when failures to redirect calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failed attempts to redirect calls exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for failures to redirect calls?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of attempts to redirect calls that failed during the monitoring period. The default is No.
Monitor Mailbox Server Access Failures	
Event Notification	
Raise event if Mailbox server access failures exceed threshold?	Select **Yes** to raise an event if the number of failed attempts to access the Mailbox server exceeds the threshold you set. The default is Yes. This script uses the value of the `Mailbox Server Access Failures` performance counter, which is the number of times the Unified Messaging system did not access a Mailbox server.
Threshold - Maximum number of Mailbox server access failures	Set the maximum number of attempts that can fail to access the Mailbox server before an event is raised. The default is 900 attempts.
Event severity when Mailbox server access failures exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failed attempts to access the Mailbox server exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for Mailbox server access failures?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of attempts to access the Mailbox server that failed during the monitoring period. The default is No.

Parameter	How to Set It
Monitor Hub Transport Server Access Failures	
Event Notification	
Raise event if Hub Transport server access failures exceed threshold?	Select **Yes** to raise an event if the number of failed attempts to access the Hub Transport server exceeds the threshold you set. The default is Yes. This script uses the value of the `Hub Transport Access Failures` performance counter, which is the number of times that attempts to access a Hub Transport server failed. This number increases only if all Hub Transport servers are unavailable.
Threshold - Maximum number of Hub Transport server access failures	Set the maximum number of attempts that can fail to access the Hub Transport server before an event is raised. The default is 900 attempts.
Event severity when Hub Transport server access failures exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failed attempts to access the Hub Transport server exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for number of Hub Transport server access failures?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of attempts to access the Hub Transport server that failed during the monitoring period. The default is No.
Monitor Active Directory Access Failures	
Event Notification	
Raise event if Active Directory access failures exceed threshold?	Select **Yes** to raise an event if the number of failed attempts to access Active Directory exceeds the threshold you set. The default is Yes. This script uses the value of the `Directory Access Failures` performance counter, which is the number of times that attempts to access Active Directory failed.
Threshold - Maximum number of Active Directory access failures	Set the maximum number of attempts that can fail to access Active Directory before an event is raised. The default is 900 attempts.
Event severity when Active Directory access failures exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of failed attempts to access Active Directory exceeds the threshold you set. The default is 5.
Data Collection	
Collect data for Active Directory access failures?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of attempts to access Active Directory that failed during the monitoring period. The default is No.

UMS_Performance

Use this Knowledge Script to monitor the performance of the Unified Messaging server: user response latency, operation response time, queued messages for call answering, queued OCS user notifications, and calls disconnected while playing audio hourglass tones. This script raises an event if a monitored value exceeds the threshold you set. In addition, this script generates data streams for monitored values.

Resource Objects

- Exchange2007_UnifiedMessagingServer
- Exchange2010_UnifiedMessagingServer

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job failure event notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UMS_Performance job fails. The default is 5.
Monitor User Response Latency	
Event Notification	
Raise event if user response latency exceeds threshold?	Select **Yes** to raise an event if the amount of time it takes for the system to respond to a user's request exceeds the threshold you set. The default is Yes. This script uses the value of the `User Response Latency` performance counter, which is the average response time, in milliseconds, for the system to respond to a user request. This average is calculated over the last 25 calls.
Threshold - Maximum user response latency	Set the maximum length of time it can take to respond to a user request before an event is raised. The default is 1 millisecond.
Event severity when user response latency exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which user response time exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for user response latency?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the average user response latency value for the monitoring period. The default is No.
Monitor Operations Response Time	
Event Notification	

Parameter	How to Set It
Raise event if percentage of operations exceeds threshold?	Select **Yes** to raise an event if Unified Messaging operations it takes a Unified Messaging operation to complete a transaction exceeds the threshold you set. The default is Yes. This script uses the `MSExchangeUMPerformance` category of performance counters.
Operations response time	Set a response time, between 2 and 6 seconds. Operations with a response time greater than this value are considered for the *Threshold - Maximum percentage of operations that exceed response time* parameter. The default is 6 seconds. The response time is the number of seconds it takes a Unified Messaging operation to complete, during which a caller is waiting for a response.
Threshold - Maximum percentage of operations that exceed the selected response time	Set the maximum percentage of operations that can exceed the response time you specify in *Operations response time*. This script raises an event if the percentage is greater than the threshold value you specify here. The default is 1%.
Event severity when percentage of operations exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which operation response time exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for percentage of operations that exceeds threshold?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns operation response time for the monitoring period. The default is No.
Monitor Call Answer Queued Messages	
Event Notification	
Raise event if call answer queued messages exceed threshold?	Select **Yes** to raise an event if the number of messages in queue to be answered exceeds the threshold you set. The default is Yes. This script uses the `Call Answer Queued Messages` performance counter, which is the number of messages created and not yet submitted for delivery.
Threshold - Maximum call answer queued messages	Set the maximum number of messages that can be in queue to be answered before an event is raised. The default is 50 messages.
Event severity when call answer queued messages exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of messages in queue to be answered exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for call answer queued messages?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of messages in queue to be answered for the monitoring period. The default is No.
Monitor Queued OCS User Event Notifications	
Event Notification	
Raise event if queued OCS user event notifications exceed threshold?	Select **Yes** to raise an event if the number of Office Communications Server notifications in queue exceeds the threshold you set. The default is Yes. This script uses the `Queued OCS User Event Notifications` performance counter, which is the number of notifications that have been created and not yet submitted for delivery.
Threshold - Maximum queued OCS user event notifications	Set the maximum number of notifications that can be in queue before an event is raised. The default is 0 notifications.

Parameter	How to Set It
Event severity when queued OCS user event notifications exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of notifications in queue exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for queued OCS user event notifications?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of notifications in queue for the monitoring period. The default is No.
Monitor Calls Disconnected During Audio Hourglass	
Event Notification	
Raise event if calls disconnected during audio hourglass exceed threshold?	Select **Yes** to raise an event if the number of calls disconnected during the audio hourglass exceeds the threshold you set. The default is Yes. This script uses the `Calls Disconnected by Callers During UM Audio Hourglass` performance counter, which is the number of calls during which the caller disconnected while Unified Messaging was playing the audio hourglass tones. Audio hourglass tones let users know they are still on hold or in queue.
Threshold - Maximum calls disconnected during audio hourglass	Set the maximum number of calls that can be disconnected during the audio hourglass before an event is raised. The default is 0 calls.
Event severity when calls disconnected during audio hourglass exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of disconnected calls exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for calls disconnected during audio hourglass?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls disconnected during audio hourglass for the monitoring period. The default is No.

Recommended Knowledge Script Group

The following Knowledge Scripts in the AppManager for Exchange2007 module are members of the Exchange2007 recommended Knowledge Script Group (KSG).

- All_BestPracticesAnalyzer
- All_ClockSynchronization
- All_EventLog
- All_ServiceStatus
- CAS_Activity
- CAS_Connectivity
- ETS_ExternalMail
- HTS_Connectivity
- MBS_MailboxAccessibility
- MBS_MailFlow
- Transport_BackPressure
- Transport_QueueStatus
- UMS_Connectivity
- UMS_Failures

You can find the Exchange2007 KSG on the RECOMMENDED tab of the Knowledge Script pane of the Operator Console.

The parameters of all scripts in the KSG are set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab, and then run the Exchange2007 group on an Exchange Server 2007 or 2010 resource.

The Exchange2007 KSG contains Knowledge Scripts for every server role. When you run the KSG on a particular server role, only the scripts in the KSG associated with that role will run. The All_* Knowledge Scripts in the KSG will run on every role.

The Exchange2007 KSG provides a "best practices" usage of AppManager for monitoring Exchange Server 2007 or 2010 in your organization. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView. For more information, see "About Policy-Based Monitoring" in the AppManager Help.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the Exchange2007 tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the Exchange2007 tab are not affected.

When deployed as part of a KSG, a script's default script parameter settings may differ from when the script is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the Exchange2007 KSG and want to restore it to its original form, you can reinstall AppManager for Exchange Server 2007 on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\Exchange2007\RECOMMENDED_Exchange2007` directory.

In addition to the Knowledge Scripts in the KSG, NetIQ Corporation recommends using the following scripts for monitoring and managing an Exchange Server 2007 or 2010 environment. The tables below summarize the scripts that are applicable for the unique elements of an Exchange Server 2007 or 2010 environment. For more information, see the AppManager Help for each script.

For performing benchmarking and trend analyses before deploying AppManager for Exchange Server 2007 and 2010, run the following scripts from the NT and AD script categories.

Recommended Knowledge Script	Description
NT_CPUByProcess	Monitors CPU usage for each process and the total CPU usage for all processes.
NT_CPULoaded	Monitors total CPU usage and queue length to determine CPU load.
NT_LogicalDiskBusy	Monitors the logical disk activity on one or more disks.
NT_LogicalDiskIO	Monitors logical disk I/O activity, including disk transfers, and reads and writes per second.
NT_MemUtil	Monitors physical memory, virtual memory, and paging files.
NT_NetworkBusy	Monitors the traffic on the network interface cards on a Windows computer.
AD_Authentications	Monitors the number of Active Directory Kerberos and NT LAN Manager (NTLM) authentications per second.

For monitoring the hardware and operating system of the Exchange Server 2007 or 2010 server and components, use the following scripts from the **NT** script category and from the categories appropriate for your hardware, such as **CIM** or **Dell**.

Recommended Knowledge Script	Description
[HardwareModule]_ ArrayPhysicalDiskStatus or ArrayPhysicalDrive	Monitors the status of physical drives in an array set.
[HardwareModule]_FanProbe or FanIndividual	Monitors the status of individual fans.
[HardwareModule]_NICError	Monitors network interface transmission errors.
[HardwareModule]_PowerSupply	Monitors the status of the hardware power supplies.
NT_CPULoaded	Monitors total CPU usage and queue length to determine CPU load.
NT_MemUtil	Monitors physical memory, virtual memory, and paging files.
NT_PhysicalDiskQLen	Monitors the number of disk jobs waiting in the queue.
NT_RunAwayProcesses	Detects runaway processes by sampling CPU usage.
NT_SystemUptime	Tracks the number of hours a computer has been operational since it was last rebooted.
NT_DNSConnectivity	Checks connectivity between a managed computer and its DNS server.

For reporting and analysis purposes, use the following script from the **NT** category.

Recommended Knowledge Script	Description
NT_SystemUptime	Tracks the number of hours a computer has been operational since it was last rebooted.

Chapter 36
Exchange-RT Knowledge Scripts

The Exchange-RT category provides the following Knowledge Scripts for monitoring the response time of Microsoft Exchange Servers.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
CheckAddressBookEntry	Checks an Exchange address book entry and reports the amount of time the operation took.
OpenFolder	Opens an Exchange folder and reports the amount of time the operation took.
OpenFolderAndRead	Opens an Exchange folder and reads the last or most recent item it contains.
SendAndReceiveMessage	Sends email from and receives it back to a specific email user account.
SendAndTrackMessage	Reports the amount of time taken to deliver an email message and return a receipt for it to the sender.
Report_Exchange-RT	Reports on availability and response time for selected Exchange Servers.

CheckAddressBookEntry

Use this Knowledge Script to check an Exchange address book entry and report the amount of time the operation took. If the transaction completes successfully, you will see a positive result for availability, even if the address book entry is not found.

If you select to use the SSL option for a test using RPC over HTTP, you must run the Knowledge Script as "Interactive User." To run using SSL, type `Interactive User` for the **Exchange Logon and Run As Username** parameter, and leave the **Password** and **Domain** parameters blank.

Note
Unlike other AppManager ResponseTime Knowledge Scripts, which require you to enter username and password information required to log into the network domain, the Exchange-RT Knowledge Scripts all use Windows NT authentication or "integrated security".

Helpful Hints

For the **Address book entry** parameter, even if the server cannot find the particular name you have entered, it still scans the address book and returns a valid response time.

If you are using a mailbox that does not have a unique name, you can do either of the following:

- Use its fully qualified name for the **Mailbox name** parameter.

  For example, say you have the following mailboxes defined on your Exchange Server: `'test'`, `'test 1'`, `'test 2'`, `'system test'`. If you specify the mail account "`test`" when creating a connection in the Microsoft Exchange Server settings dialog box on your Exchange test client, you are prompted for the mailbox to use. The fully qualified name for '`test`' would be in the format: `/o=Your Corporation/ou=Your City/cn=Recipients/cn=test.` Supply this value for the **Mailbox name** parameter.

  To determine the fully qualified mailbox name, click **Check Name** when configuring Exchange Server settings on the test client. A dialog box allows you to specify the account to use. Highlight the desired account and click **Properties**. The value in the **Email address** field is the string to use in the Exchange Service Connection **mailbox** field.

- Enable the **Resolve and use Exchange distinguished name** parameter.

  If the value specified for the **Mailbox name** is ambiguous, for example, because the names of multiple mailboxes are very similar, the Exchange Server may not be able to determine which mailbox to use in the response-time test. When you enable the **Resolve and use Exchange distinguished name** parameter, the ResponseTime for Exchange managed object resolves the name in Active Directory to the first match found and uses that value for the transaction.

Collecting Data

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to 6 response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. For more information, see "Setting Parameter Values" on page 2031.

- **Availability**–Returns one of the following values:
  - 1 or 100 – the transaction was successful
  - 0 – the transaction was not successful

  The Availability data point is an indication of whether the test succeeded or failed. If, for example, a connection to the Exchange Server was established but the mailbox failed to open, the Availability data point will be 0 (not available, or not successful).

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The Exchange-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is not generated.
- The transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. For more information, see the description of the **Event on** parameter, below.

Resource Objects

Exchange response time clients (Exchange-RT)

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect availability data for graphs and reports. By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Exchange used a 0 ("not available") or 1 ("available") format to indicate availability that is, test success or failure. You now have the option to use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, an event is raised.
Event severity when transaction fails	If events are enabled, set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect response-time data for graphs and reports. By default, data is collected.

Description	How to Set It
Include time to resolve distinguished name?	Select **Yes** to add extra time to resolve the distinguished name of the account. In some cases, resolving distinguished names could affect performance. If you want to collect this data, enable this parameter and the Collect data for resolving distinguished name? parameter. This parameter is disabled by default.
Include time to create profile in response time?	Select the **Yes** check box to include the time taken to create the Exchange profile in the response-time calculation. By default, the time to create the profile is not included in the response time.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The event message contains a breakdown of the total response time. The default is 15 seconds.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the response-time threshold is exceeded. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15.
Response Time Breakdown	
Collect data for resolving distinguished name?	Select **Yes** to collect the results of resolving the distinguished name. By default, this information is not collected.
Collect data for initializing Exchange?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to initialize the connection to the Exchange server. By default, separate response-time data streams are not collected.
Collect data for creating Exchange profile?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to create the Exchange profile. By default, separate response-time data streams are not collected.
Collect data for logon?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to log on to the Exchange server. By default, separate response-time data streams are not collected.
Collect data for opening Exchange database?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the Exchange database. By default, separate response-time data streams are not collected.
Collect data for opening address book?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the Outlook address book. By default, separate response-time data streams are not collected.
Collect data for resolving entry?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to resolve the Outlook address book entry. By default, separate response-time data streams are not collected.
Address book entry	Enter the address-book entry to check in the response-time test--the name of a person in the Exchange address book. Use the following syntax: For example: `John Doe` If you are setting the **Event on** parameter, the **Address book entry** parameter lets you select the computer where the event will appear in your console. Enter the name of the server, or click the browse button ([**...**]) to select from a list of available servers. The computer you select must already be in the TreeView.

Description	How to Set It
Event on	Select the TreeView location where events should be displayed. Select either: • Agent. The client computer in the response-time tests. This is the default. • Server. The Exchange server being tested--see the **Exchange server name** parameter, below. • Both. The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Exchange Server Settings	
Exchange server name	Enter the name of the Exchange server.
Mailbox name	Enter the name of the mailbox, which is usually a username.
Resolve and use Exchange distinguished name?	Select the **Yes** check box to instruct the ResponseTime for Exchange managed object to resolve the name in Active Directory to the first match found and use that value for the transaction. This option is helpful if the name you supplied for the **Mailbox name** parameter is ambiguous. For example, there are mailboxes with names so similar that the Exchange Server cannot determine which one to use for the test. By default, the DN for the mailbox is not used.
Using RPC over HTTP	
Connect to Exchange Server using HTTP?	Select the **Yes** check box to use the hypertext transfer protocol (HTTP) to make the connection to the server that is acting as the RPC proxy for the Exchange server. If enabled, allows you to test Exchange server response time in a proxy situation by using a remote procedure call (RPC) sent over HTTP. By default, HTTP is not used to connect to the Exchange server.
URL to connect to proxy server for Exchange	Enter the URL of the Exchange Server computer that is configured as an RPC proxy server. The RPC proxy server communicates with clients seeking access to the Exchange server. Use the following format: For example: `exchproxy01.netiq.com` Required if RPC over HTTP is used.
SSL Settings	
Connect using SSL only	Select the **Yes** check box to use the Secure Sockets Layer (SSL) security protocol to secure the HTTP connection to the proxy Exchange Server. If you select to use the SSL option for a test using RPC over the HTTP protocol, you must run the Knowledge Script as “Interactive User” due to the security requirements of SSL. For more information, see the **Username** parameter below. By default, SSL is not used for the connection.
Mutually authenticate the session when connecting	Select the **Yes** check box to require the client computer and the Exchange server to perform authentication when the Knowledge Script requests the connection to the Exchange server. By default, authentication is not performed.

Description	How to Set It
Principal name for proxy server	The service principal name of the proxy Exchange server service. This name must be recognized as an entity by the SSL server. The format is `msstd:FQDN` where FQDN is the fully-qualified domain name of the proxy server. Required if the previous parameter (**Mutually authenticate...**) is enabled.
On fast networks, connect using HTTP first, then connect using TCP/IP	Select the **Yes** check box to attempt the connection to the proxy Exchange Server using the HTTP protocol first, and then, if the connection attempt fails, to use TCP/IP for the connection. This setting affects connection response times on fast networks, which Outlook defines as faster than 128 kilobits per second (Kbps). By default, this option is disabled on fast networks.
On slow networks, connect using HTTP first, then connect using TCP/IP	Select the **Yes** check box to attempt the connection to the proxy Exchange Server using the HTTP protocol first, and then, if the connection attempt fails, to use TCP/IP for the connection. This setting affects connection response times on slow networks, which Outlook defines as slower than or equal to 128 kilobits per second (Kbps). By default, this option is enabled on slow networks.
Exchange Logon and Run As	
Username	Enter the name of the person who owns or is authorized to access the mailbox. If you select to use the SSL option for a test using RPC over HTTP, you must run the Knowledge Script as “Interactive User”. Running as “Interactive User” requires that a user be physically logged into the managed client. To run using SSL, type `Interactive User` here. Leave the **Password** and **Domain** parameters blank.
Password	Enter the password associated with this user that is required to log on to the network and run the application. Leave blank to run as Interactive User.
Domain	Enter the domain associated with this user--the domain name you are logging onto. Leave blank to run as Interactive User.
Administrators group on managed client	Enter the name of the Administrators Group on the managed client. Typically, this name is “Administrators”. The default is “`Administrators`”.
Timeouts	
Job timeout	Set the timeout value, from 1 to 900 seconds, to determine the maximum time allowed to process a job before it's aborted. When an Exchange-RT Knowledge Script job runs, a job timer is started. If the transaction takes longer than the Job timeout, the transaction is stopped and a “Job Timeout" event is raised. The default is 120 seconds.
Queue timeout	Set the timeout value, from 1 to 1200 seconds, to determine how long a job can wait for resources before it's aborted. Multiple simultaneous Exchange-RT Knowledge Script jobs must wait for a token to run. If no token is available for a job you're trying to run, the job is added to the queue and starts a queue timer. When the Queue Timeout for a job expires, the job does not run, a "Queue Timeout" event is raised, and the job is moved to the end of the queue. The default is 300 seconds.

OpenFolder

Use this Knowledge Script to open a specified Exchange folder and report the amount of time the operation took. The selected folder can be either public or private.

If you select to use the SSL option for a test using RPC over HTTP, you must run the Knowledge Script as "Interactive User." To run using SSL, type `Interactive User` for the **Exchange Logon and Run As Username** parameter, and leave the **Password** and **Domain** parameters blank.

Helpful Hints

- If you are using a mailbox that does not have a unique name, you should either enable the **Resolve and use Exchange distinguished name?** parameter or supply the fully qualified name for the mailbox. For more information, see the "Helpful Hints" section of "CheckAddressBookEntry" on page 2030.
- The folder name that you must specify in this Knowledge Script can be for either a private or public folder. The **Folder access** parameter lets you indicate which type you have selected.

Collecting Data

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to 5 response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. For more information, see "Setting Parameter Values" on page 2036.
- **Availability**–Returns one of the following values:
  - 1 or 100 – the test was successful
  - 0 – the test was not successful
- The Availability data point is an indication of whether the test succeeded or failed. If, for example, a connection to the Exchange Server was established but the mailbox failed to open, the Availability data point will be 0 (not available, or not successful).

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The Exchange-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is not generated.
- The transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. For more information, see the description of the **Event on** parameter, below.

Resource Objects

Exchange response time clients (Exchange-RT)

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect availability data for graphs and reports. By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Exchange used a 0 ("not available") or 1 ("available") format to indicate availability that is, test success or failure. You now have the option to use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, an event is raised.
Event severity when transaction fails	If events are enabled, set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect response-time data for graphs and reports. By default, data is collected.
Include time to create profile in response time?	Select the **Yes** check box to include the time taken to create the Exchange profile in the response-time calculation. By default, the time to create the profile is not included in the response time.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The event message contains a breakdown of the total response time. The default is 15 seconds.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the response-time threshold is exceeded. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15.
Response Time Breakdown	
Collect data for initializing Exchange?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to initialize the connection to the Exchange server. By default, separate response-time data streams are not collected.
Collect data for creating Exchange profile?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to create the Exchange profile. By default, separate response-time data streams are not collected.
Collect data for logon?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to log on to the Exchange server. By default, separate response-time data streams are not collected.
Collect data for opening Exchange database?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the Exchange database. By default, separate response-time data streams are not collected.

Description	How to Set It
Collect data for opening folder?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the specified folder. By default, separate response-time data streams are not collected.
Folder name	The name of the Exchange folder to open. The default is `Inbox`. If you are setting the **Event on** parameter, the **Folder name** parameter lets you select the Exchange folder where any events will appear in your console.
Folder access	The security status of the folder. Select either `Private` or `Public`. Default is `Private`.
Event on	Select the TreeView location where events should be displayed. Select either: • Agent. The client computer in the response-time tests; corresponds to the Exchange folder you selected for the **Folder name** parameter, above. This is the default. • Server. The Exchange server being tested--see the **Exchange server name** parameter. • Both. The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Exchange Server Settings	
Exchange server name	Enter the name of the Exchange server, or click the browse button ([**...**]) to select from a list of available servers. The servers in the list are already in the TreeView.
Mailbox name	Enter the name of the mailbox, which is usually a username.
Resolve and use Exchange distinguished name?	Select the **Yes** check box to instruct the ResponseTime for Exchange managed object to resolve the name in Active Directory to the first match found and use that value for the transaction. This option is helpful if the name you supplied for the **Mailbox name** parameter is ambiguous. For example, there are mailboxes with names so similar that the Exchange Server cannot determine which one to use for the test. By default, the DN for the mailbox is not used.
Using RPC over HTTP	
Connect to Exchange Server using HTTP?	Select the **Yes** check box to use the hypertext transfer protocol (HTTP) to make the connection to the server that is acting as the RPC proxy for the Exchange server. If enabled, allows you to test Exchange server response time in a proxy situation by using a remote procedure call (RPC) sent over HTTP. By default, HTTP is not used to connect to the Exchange server.
URL to connect to proxy server for Exchange	Enter the URL of the Exchange Server computer that is configured as an RPC proxy server. The RPC proxy server communicates with clients seeking access to the Exchange server. Use the following format. For example: `exchproxy01.netiq.com` Required if RPC over HTTP is used.
SSL Settings	

Description	How to Set It
Connect using SSL only	Select the **Yes** check box to use the Secure Sockets Layer (SSL) security protocol to secure the HTTP connection to the proxy Exchange Server. If you select to use the SSL option for a test using RPC over the HTTP protocol, you must run the Knowledge Script as “Interactive User” due to the security requirements of SSL. See the **Username** parameter below for more information. By default, SSL is not used for the connection.
Mutually authenticate the session when connecting	Select the **Yes** check box to require the client computer and the Exchange server to perform authentication when the Knowledge Script requests the connection to the Exchange server. By default, authentication is not performed.
Principal name for proxy server	The service principal name of the proxy Exchange server service. This name must be recognized as an entity by the SSL server. The format is `msstd:FQDN` where FQDN is the fully-qualified domain name of the proxy server. Required if the previous parameter (**Mutually authenticate...**) is enabled.
On fast networks, connect using HTTP first, then connect using TCP/IP	Select the **Yes** check box to attempt the connection to the proxy Exchange Server using the HTTP protocol first, and then, if the connection attempt fails, to use TCP/IP for the connection. This setting affects connection response times on fast networks, which Outlook defines as faster than 128 kilobits per second (Kbps). By default, this option is disabled on fast networks.
On slow networks, connect using HTTP first, then connect using TCP/IP	Select the **Yes** check box to attempt the connection to the proxy Exchange Server using the HTTP protocol first, and then, if the connection attempt fails, to use TCP/IP for the connection. This setting affects connection response times on slow networks, which Outlook defines as slower than or equal to 128 kilobits per second (Kbps). By default, this option is enabled on slow networks.
Exchange Logon and Run As	
Username	Enter the name of the person who owns or is authorized to access the mailbox. If you select to use the SSL option for a test using RPC over HTTP, you must run the Knowledge Script as “Interactive User”. Running as “Interactive User” requires that a user be physically logged into the managed client. To run using SSL, type `Interactive User` here. Leave the **Password** and **Domain** parameters blank.
Password	Enter the password associated with this user that is required to log on to the network and run the application. Leave blank to run as Interactive User.
Domain	Enter the domain associated with this user--the domain name you are logging onto. Leave blank to run as Interactive User.
Administrators group on managed client	Enter the name of the Administrators Group on the managed client. Typically, this name is “Administrators”. The default is “`Administrators`”.
Timeouts	
Job timeout	Set the timeout value, from 1 to 900 seconds, to determine the maximum time allowed to process a job before it's aborted. When an Exchange-RT Knowledge Script job runs, a job timer is started. If the transaction takes longer than the Job timeout, the transaction is stopped and a “Job Timeout" event is raised. The default is 120 seconds.

Description	How to Set It
Queue timeout	Set the timeout value, from 1 to 1200 seconds, to determine how long a job can wait for resources before it's aborted. Multiple simultaneous Exchange-RT Knowledge Script jobs must wait for a token to run. If no token is available for a job you're trying to run, the job is added to the queue and starts a queue timer. When the Queue Timeout for a job expires, the job does not run, a "Queue Timeout" event is raised, and the job is moved to the end of the queue. The default is 300 seconds.

OpenFolderAndRead

Use this Knowledge Script to open an Exchange folder and read the last or most recent item it contains.

This script does not return an error if the folder is empty, and the job will complete normally.

If you select to use the SSL option for a test using RPC over HTTP, you must run the Knowledge Script as "Interactive User." To run using SSL, type `Interactive User` for the **Exchange Logon and Run As Username** parameter, and leave the **Password** and **Domain** parameters blank.

Helpful Hints

- If you are using a mailbox that does not have a unique name, you should either enable the **Resolve and use Exchange distinguished name?** parameter or supply the fully qualified name for the mailbox. For more information, see the "Helpful Hints" section of "CheckAddressBookEntry" on page 2030.
- The folder name that you must specify in this Knowledge Script can be for either a private or public folder. The **Folder access** parameter lets you indicate which type you have selected.

Collecting Data

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to 6 response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. For more information, see "Setting Parameter Values" on page 2041.
- **Availability**–Returns one of the following values:
  - 1 or 100 – the test was successful
  - 0 – the test was not successful
- The Availability data point is an indication of whether the test succeeded or failed. If, for example, a connection to the Exchange Server was established but the mailbox failed to open, the Availability data point will be 0 (not available, or not successful).

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The Exchange-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is not generated.
- The transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. For more information, see the description of the **Event on** parameter, below.

Resource Objects

Exchange response time clients (Exchange-RT)

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect availability data for graphs and reports. By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Exchange used a 0 ("not available") or 1 ("available") format to indicate availability that is, test success or failure. You now have the option to use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, an event is raised.
Event severity when transaction fails	If events are enabled, set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect response-time data for graphs and reports. By default, data is collected.
Include time to create profile in response time?	Select the **Yes** check box to include the time taken to create the Exchange profile in the response-time calculation. By default, the time to create the profile is not included in the response time.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The event message contains a breakdown of the total response time. The default is 15 seconds.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the response-time threshold is exceeded. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15.
Response Time Breakdown	
Collect data for initializing Exchange?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to initialize the connection to the Exchange server. By default, separate response-time data streams are not collected.
Collect data for creating Exchange profile?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to create the Exchange profile. By default, separate response-time data streams are not collected.
Collect data for logon?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to log on to the Exchange server. By default, separate response-time data streams are not collected.
Collect data for opening Exchange database?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the Exchange database. By default, separate response-time data streams are not collected.

Description	How to Set It
Collect data for opening folder?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the folder. By default, separate response-time data streams are not collected.
Collect data for reading the last folder item?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to read the last item received in the folder. By default, separate response-time data streams are not collected.
Folder name	The name of the Exchange folder to open. The default is `Inbox`. If you are setting the **Event on** parameter, the **Folder name** parameter lets you select the Exchange folder where any events will appear in your console.
Folder access	The security status of the folder. Select either `Private` or `Public`. Default is `Private`.
Event on	Select the TreeView location where events should be displayed. Select either: • Agent. The client computer in the response-time tests; corresponds to the Exchange folder you selected for the **Folder name** parameter. This is the default. • Server. The Exchange server being tested--see the **Exchange server name** parameter. • Both. The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Exchange Server Settings	
Exchange server name	Enter the name of the Exchange server, or click the browse button ([**...**]) to select from a list of available servers. The servers in the list are already in the TreeView.
Mailbox name	Enter the name of the mailbox, which is usually a username.
Resolve and use Exchange distinguished name?	Select the **Yes** check box to instruct the ResponseTime for Exchange managed object to resolve the name in Active Directory to the first match found and use that value for the transaction. This option is helpful if the name you supplied for the **Mailbox name** parameter is ambiguous. For example, there are mailboxes with names so similar that the Exchange Server cannot determine which one to use for the test. By default, the DN for the mailbox is not used.
Using RPC over HTTP	
Connect to Exchange Server using HTTP?	Select the **Yes** check box to use the hypertext transfer protocol (HTTP) to make the connection to the server that is acting as the RPC proxy for the Exchange server. If enabled, allows you to test Exchange server response time in a proxy situation by using a remote procedure call (RPC) sent over HTTP. By default, HTTP is not used to connect to the Exchange server.

Description	How to Set It
URL to connect to proxy server for Exchange	Enter the URL of the Exchange Server computer that is configured as an RPC proxy server. The RPC proxy server communicates with clients seeking access to the Exchange server. Use the following format. For example: `exchproxy01.netiq.com` Required if RPC over HTTP is used.
SSL Settings	
Connect using SSL only	Select the **Yes** check box to use the Secure Sockets Layer (SSL) security protocol to secure the HTTP connection to the proxy Exchange Server. If you select to use the SSL option for a test using RPC over the HTTP protocol, you must run the Knowledge Script as “Interactive User” due to the security requirements of SSL. For more information, see the **Username** parameter below. By default, SSL is not used for the connection.
Mutually authenticate the session when connecting	Select the **Yes** check box to require the client computer and the Exchange server to perform authentication when the Knowledge Script requests the connection to the Exchange server. By default, authentication is not performed.
Principal name for proxy server	The service principal name of the proxy Exchange server service. This name must be recognized as an entity by the SSL server. The format is `msstd:FQDN` where FQDN is the fully-qualified domain name of the proxy server. Required if the previous parameter (**Mutually authenticate...**) is enabled.
On fast networks, connect using HTTP first, then connect using TCP/IP	Select the **Yes** check box to attempt the connection to the proxy Exchange Server using the HTTP protocol first, and then, if the connection attempt fails, to use TCP/IP for the connection. This setting affects connection response times on fast networks, which Outlook defines as faster than 128 kilobits per second (Kbps). By default, this option is disabled on fast networks.
On slow networks, connect using HTTP first, then connect using TCP/IP	Select the **Yes** check box to attempt the connection to the proxy Exchange Server using the HTTP protocol first, and then, if the connection attempt fails, to use TCP/IP for the connection. This setting affects connection response times on slow networks, which Outlook defines as slower than or equal to 128 kilobits per second (Kbps). By default, this option is enabled on slow networks.
Exchange Logon and Run As	
Username	Enter the name of the person who owns or is authorized to access the mailbox. If you select to use the SSL option for a test using RPC over HTTP, you must run the Knowledge Script as “Interactive User". Running as “Interactive User” requires that a user be physically logged into the managed client. To run using SSL, type `Interactive User` here. Leave the **Password** and **Domain** parameters blank.
Password	Enter the password associated with this user that is required to log on to the network and run the application. Leave blank to run as Interactive User.
Domain	Enter the domain associated with this user--the domain name you are logging onto. Leave blank to run as Interactive User.
Administrators group on managed client	Enter the name of the Administrators Group on the managed client. Typically, this name is “Administrators”. The default is “`Administrators`”.
Timeouts	

Description	How to Set It
Job timeout	Set the timeout value, from 1 to 900 seconds, to determine the maximum time allowed to process a job before it's aborted. When an Exchange-RT Knowledge Script job runs, a job timer is started. If the transaction takes longer than the Job timeout, the transaction is stopped and a “Job Timeout" event is raised. The default is 120 seconds.
Queue timeout	Set the timeout value, from 1 to 1200 seconds, to determine how long a job can wait for resources before it's aborted. Multiple simultaneous Exchange-RT Knowledge Script jobs must wait for a token to run. If no token is available for a job you're trying to run, the job is added to the queue and starts a queue timer. When the Queue Timeout for a job expires, the job does not run, a "Queue Timeout" event is raised, and the job is moved to the end of the queue. The default is 300 seconds.

SendAndReceiveMessage

Use this Knowledge Script to send email from and receive it back to a specific email user account. For testing purposes, the server is sending a message to itself. It reports the operation time.

The incoming message header contains a unique identifier that tracks and identifies the message. If the message is received that matches the sent message within the timeout time, the message is then deleted. If the timeout occurs before the message is received, the message displays in the Outlook Inbox.

If you select to use the SSL option for a test using RPC over HTTP, you must run the Knowledge Script as "Interactive User." To run using SSL, type `Interactive User` for the **Exchange Logon and Run As Username** parameter, and leave the **Password** and **Domain** parameters blank.

Tip
If you are using a mailbox that does not have a unique name, you should either enable the Resolve and use Exchange distinguished name? parameter or supply the fully qualified name for the mailbox. For more information, see the "Helpful Hints" section of "CheckAddressBookEntry" on page 2030.

Collecting Data

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Response time.**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to 11 response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. For more information, see "Setting Parameter Values" on page 2046.
- **Availability**–Returns one of the following values:
  - 1 or 100 – the test was successful
  - 0 – the test was not successful
- The Availability data point is an indication of whether the test succeeded or failed. If, for example, a connection to the Exchange Server was established but the mailbox failed to open, the Availability data point will be 0 (not available, or not successful).

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The Exchange-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is not generated.
- The transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. For more information, see the description of the **Event on** parameter, below.

Resource Objects

Exchange response time clients (Exchange-RT)

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect availability data for graphs and reports. By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Exchange used a 0 ("not available") or 1 ("available") format to indicate availability that is, test success or failure. You now have the option to use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, an event is raised.
Event severity when transaction fails	If events are enabled, set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect response-time data for graphs and reports. By default, data is collected.
Include time to create profile in response time?	Select the **Yes** check box to include the time taken to create the Exchange profile in the response-time calculation. By default, the time to create the profile is not included in the response time.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The event message contains a breakdown of the total response time. The default is 15 seconds.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the response-time threshold is exceeded. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15.
Response Time Breakdown	
Collect data for initializing Exchange?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to initialize the connection to the Exchange server. By default, separate response-time data streams are not collected.
Collect data for creating Exchange profile?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to create the Exchange profile. By default, separate response-time data streams are not collected.
Collect data for logon?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to log on to the Exchange server. By default, separate response-time data streams are not collected.
Collect data for opening Exchange database?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the Exchange database. By default, separate response-time data streams are not collected.

Description	How to Set It
Collect data for opening address book?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the Outlook address book. By default, separate response-time data streams are not collected.
Collect data for opening Inbox?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the Inbox. By default, separate response-time data streams are not collected.
Collect data for opening Outbox?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the Outbox. By default, separate response-time data streams are not collected.
Collect data for creating message?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to create the test email message. By default, separate response-time data streams are not collected.
Collect data for resolving recipient name?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to resolve the name of the recipient of the test email message. For more information, see the **Mailbox name** parameter, below. By default, separate response-time data streams are not collected.
Collect data for sending message?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to actually send the test email message. By default, separate response-time data streams are not collected.
Collect data for waiting until message shows up in Inbox?	Select the **Yes** check box to collect a separate response-time data stream for the time taken for the test message to show up in the recipient's mailbox. By default, separate response-time data streams are not collected.
Message size	Enter the size of the message in bytes. Default is 100.
Event on	Select the TreeView location where events should be displayed. Select either: • Agent. The client computer in the response-time tests. This is the default. • Server. The Exchange server being tested--see the **Exchange server name** parameter. • Both. The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Exchange Server Settings	
Exchange server name	Enter the name of the Exchange server, or click the browse button ([**...**]) to select from a list of available servers. The servers in the list are already in the TreeView.
Mailbox name	Enter the name of the mailbox, which is usually a username.
Resolve and use Exchange distinguished name?	Select the **Yes** check box to instruct the ResponseTime for Exchange managed object to resolve the name in Active Directory to the first match found and use that value for the transaction. This option is helpful if the name you supplied for the **Mailbox name** parameter is ambiguous. For example, there are mailboxes with names so similar that the Exchange Server cannot determine which one to use for the test. By default, the DN for the mailbox is not used.
Using RPC over HTTP	

Description	How to Set It
Connect to Exchange Server using HTTP?	Select the **Yes** check box to use the hypertext transfer protocol (HTTP) to make the connection to the server that is acting as the RPC proxy for the Exchange server. If enabled, allows you to test Exchange server response time in a proxy situation by using a remote procedure call (RPC) sent over HTTP. By default, HTTP is not used to connect to the Exchange server.
URL to connect to proxy server for Exchange	Enter the URL of the Exchange Server computer that is configured as an RPC proxy server. The RPC proxy server communicates with clients seeking access to the Exchange server. Use the following format. For example: `exchproxy01.netiq.com` Required if RPC over HTTP is used.
SSL Settings	
Connect using SSL only	Select the **Yes** check box to use the Secure Sockets Layer (SSL) security protocol to secure the HTTP connection to the proxy Exchange Server. If you select to use the SSL option for a test using RPC over the HTTP protocol, you must run the Knowledge Script as “Interactive User” due to the security requirements of SSL. For more information, see the **Username** parameter below. By default, SSL is not used for the connection.
Mutually authenticate the session when connecting	Select the **Yes** check box to require the client computer and the Exchange server to perform authentication when the Knowledge Script requests the connection to the Exchange server. By default, authentication is not performed.
Principal name for proxy server	The service principal name of the proxy Exchange server service. This name must be recognized as an entity by the SSL server. The format is `msstd:FQDN` where FQDN is the fully-qualified domain name of the proxy server. Required if the previous parameter (**Mutually authenticate...**) is enabled.
On fast networks, connect using HTTP first, then connect using TCP/IP	Select the **Yes** check box to attempt the connection to the proxy Exchange Server using the HTTP protocol first, and then, if the connection attempt fails, to use TCP/IP for the connection. This setting affects connection response times on fast networks, which Outlook defines as faster than 128 kilobits per second (Kbps). By default, this option is disabled on fast networks.
On slow networks, connect using HTTP first, then connect using TCP/IP	Select the **Yes** check box to attempt the connection to the proxy Exchange Server using the HTTP protocol first, and then, if the connection attempt fails, to use TCP/IP for the connection. This setting affects connection response times on slow networks, which Outlook defines as slower than or equal to 128 kilobits per second (Kbps). By default, this option is enabled on slow networks.
Exchange Logon and Run As	
Username	Enter the name of the person who owns or is authorized to access the mailbox. If you select to use the SSL option for a test using RPC over HTTP, you must run the Knowledge Script as “Interactive User”. Running as “Interactive User” requires that a user be physically logged into the managed client. To run using SSL, type `Interactive User` here. Leave the **Password** and **Domain** parameters blank.
Password	Enter the password associated with this user that is required to log on to the network and run the application. Leave blank to run as Interactive User.

Description	How to Set It
Domain	Enter the domain associated with this user--the domain name you are logging onto. Leave blank to run as Interactive User.
Administrators group on managed client	Enter the name of the Administrators Group on the managed client. Typically, this name is “Administrators”. The default is “`Administrators`”.
Timeouts	
Message delivery timeout	Enter the time, in seconds, for the job to wait for the tracking message to show up in the mailbox before the job is aborted. Enter a value from 1 to 600 seconds. The default is 75 seconds.
Job timeout	Set the timeout value, from 1 to 900 seconds, to determine the maximum time allowed to process a job before it's aborted. When an Exchange-RT Knowledge Script job runs, a job timer is started. If the transaction takes longer than the Job timeout, the transaction is stopped and a “Job Timeout" event is raised. The default is 90 seconds.
Queue timeout	Set the timeout value, from 1 to 1200 seconds, to determine how long a job can wait for resources before it's aborted. Multiple simultaneous Exchange-RT Knowledge Script jobs must wait for a token to run. If no token is available for a job you're trying to run, the job is added to the queue and starts a queue timer. When the Queue Timeout for a job expires, the job does not run, a "Queue Timeout" event is raised, and the job is moved to the end of the queue. The default is 120 seconds.

SendAndTrackMessage

An Outlook user sending an email message can track the delivery time by requesting a message delivery receipt. Use this Knowledge Script to find out the time required to send an email message and to return a receipt for that email message back to the sender.

Note
The recipient email address must reside on an Exchange server. If the server is not an Exchange server, a delivery receipt is not delivered and a timeout occurs.

This Knowledge Script sends the message with a delivery notification flag to a selected mailbox. The message that was sent remains in the Inbox of the recipient. Although this Knowledge Script cannot delete the test messages from the recipient's Inbox, AppManager ResponseTime for Exchange removes the delivery notification that appears in the sender's Inbox if the test message is delivered, and if the notification is received, before the configured **Job timeout** expires. To retrieve the test message, the script looks at the subject for a unique identifier that matches one applied to the sent message.

The receiving user will have test email messages in his or her Inbox that cannot be deleted by this Knowledge Script. NetIQ Corporation recommends that you create a rule in Microsoft Exchange to delete those test messages periodically.

If you select to use the SSL option for a test using RPC over HTTP, you must run the Knowledge Script as "Interactive User." To run using SSL, type `Interactive User` for the **Exchange Logon and Run As Username** parameter, and leave the **Password** and **Domain** parameters blank.

Tip
If you are using a mailbox that does not have a unique name, you should either enable the Resolve and use Exchange distinguished name? parameter or supply the fully qualified name for the mailbox. For more information, see the "Helpful Hints" section of "CheckAddressBookEntry" on page 2030.

Collecting Data

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Response time.**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to 11 response-time breakdown data streams can be collected. These are individual data points for the different parts of the Knowledge Script transaction that are timed. For more information, see "Setting Parameter Values" on page 2051.
- **Availability**–Returns one of two values:
  - 1 – the test was successful
  - 0 – the test was not successful
- The Availability data point is an indication of whether the test succeeded or failed. If, for example, a connection to the Exchange Server was established but the mailbox failed to open, the Availability data point will be 0 (not available, or not successful).

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.

- The Exchange-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is not generated.
- The transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. For more information, see the description of the **Event on** parameter, below.

Resource Objects

Exchange response time clients (Exchange-RT)

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect availability data for graphs and reports. By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Exchange used a 0 ("not available") or 1 ("available") format to indicate availability that is, test success or failure. You now have the option to use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, an event is raised.
Event severity when transaction fails	If events are enabled, set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect response-time data for graphs and reports. By default, data is collected.
Include time to create profile in response time?	Select the **Yes** check box to include the time taken to create the Exchange profile in the response-time calculation. By default, the time to create the profile is not included in the response time.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The event message contains a breakdown of the total response time. The default is 15 seconds.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the response-time threshold is exceeded. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15.

Description	How to Set It
Response Time Breakdown	
Collect data for initializing Exchange?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to initialize the connection to the Exchange server. By default, separate response-time data streams are not collected.
Collect data for creating Exchange profile?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to create the Exchange profile. By default, separate response-time data streams are not collected.
Collect data for logon?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to log on to the Exchange server. By default, separate response-time data streams are not collected.
Collect data for opening Exchange database?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the Exchange database. By default, separate response-time data streams are not collected.
Collect data for opening address book?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the Outlook address book. By default, separate response-time data streams are not collected.
Collect data for opening Inbox?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the Inbox. By default, separate response-time data streams are not collected.
Collect data for opening Outbox?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to open the Outbox. By default, separate response-time data streams are not collected.
Collect data for creating message?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to create the test email message. By default, separate response-time data streams are not collected.
Collect data for resolving recipient name?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to resolve the name of the recipient of the test email message. For more information, see the **Mailbox name** parameter, below. By default, separate response-time data streams are not collected.
Collect data for sending message?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to actually send the test email message. By default, separate response-time data streams are not collected.
Collect data for waiting until tracking message shows up in Inbox?	Select the **Yes** check box to collect a separate response-time data stream for the time taken for the test message to show up in the recipient's mailbox. By default, separate response-time data streams are not collected.
Email address	Enter the address the message is being sent to on an Exchange server.
Message size	Enter the size of the message in bytes. Default is 100.
Event on	Select the TreeView location where events should be displayed. Select either: • Agent. The client computer in the response-time tests. This is the default. • Server. The Exchange server being tested--see the **Exchange server name** parameter. • Both. The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Exchange Server Settings	

Description	How to Set It
Exchange server name	Enter the name of the Exchange server, or click the browse button ([**...**]) to select from a list of available servers. The servers in the list are already in the TreeView.
Mailbox name	Enter the name of the mailbox, which is usually a username.
Resolve and use Exchange distinguished name?	Select the **Yes** check box to instruct the ResponseTime for Exchange managed object to resolve the name in Active Directory to the first match found and use that value for the transaction. This option is helpful if the name you supplied for the **Mailbox name** parameter is ambiguous. For example, there are mailboxes with names so similar that the Exchange Server cannot determine which one to use for the test. By default, the DN for the mailbox is not used.
Using RPC over HTTP	
Connect to Exchange Server using HTTP?	Select the **Yes** check box to use the hypertext transfer protocol (HTTP) to make the connection to the server that is acting as the RPC proxy for the Exchange server. If enabled, allows you to test Exchange server response time in a proxy situation by using a remote procedure call (RPC) sent over HTTP. By default, HTTP is not used to connect to the Exchange server.
URL to connect to proxy server for Exchange	Enter the URL of the Exchange Server computer that is configured as an RPC proxy server. The RPC proxy server communicates with clients seeking access to the Exchange server. Use the following format. For example: `exchproxy01.netiq.com` Required if RPC over HTTP is used.
SSL Settings	
Connect using SSL only	Select the **Yes** check box to use the Secure Sockets Layer (SSL) security protocol to secure the HTTP connection to the proxy Exchange Server. If you select to use the SSL option for a test using RPC over the HTTP protocol, you must run the Knowledge Script as “Interactive User” due to the security requirements of SSL. For more information, see the **Username** parameter below. By default, SSL is not used for the connection.
Mutually authenticate the session when connecting	Select the **Yes** check box to require the client computer and the Exchange server to perform authentication when the Knowledge Script requests the connection to the Exchange server. By default, authentication is not performed.
Principal name for proxy server	The service principal name of the proxy Exchange server service. This name must be recognized as an entity by the SSL server. The format is `msstd:FQDN` where FQDN is the fully-qualified domain name of the proxy server. Required if the previous parameter (**Mutually authenticate...**) is enabled.
On fast networks, connect using HTTP first, then connect using TCP/IP	Select the **Yes** check box to attempt the connection to the proxy Exchange Server using the HTTP protocol first, and then, if the connection attempt fails, to use TCP/IP for the connection. This setting affects connection response times on fast networks, which Outlook defines as faster than 128 kilobits per second (Kbps). By default, this option is disabled on fast networks.

Description	How to Set It
On slow networks, connect using HTTP first, then connect using TCP/IP	Select the **Yes** check box to attempt the connection to the proxy Exchange Server using the HTTP protocol first, and then, if the connection attempt fails, to use TCP/IP for the connection. This setting affects connection response times on slow networks, which Outlook defines as slower than or equal to 128 kilobits per second (Kbps). By default, this option is enabled on slow networks.
Exchange Logon and Run As	
Username	Enter the name of the person who owns or is authorized to access the mailbox. If you select to use the SSL option for a test using RPC over HTTP, you must run the Knowledge Script as “Interactive User”. Running as “Interactive User” requires that a user be physically logged into the managed client. To run using SSL, type `Interactive User` here. Leave the **Password** and **Domain** parameters blank.
Password	Enter the password associated with this user that is required to log on to the network and run the application. Leave blank to run as Interactive User.
Domain	Enter the domain associated with this user--the domain name you are logging onto. Leave blank to run as Interactive User.
Administrators group on managed client	Enter the name of the Administrators Group on the managed client. Typically, this name is “Administrators”. The default is “`Administrators`”.
Timeouts	
Message delivery timeout	Enter the time, in seconds, for the job to wait for the tracking message to show up in the mailbox before the job is aborted. Enter a value from 1 to 600 seconds. The default is 75 seconds.
Job timeout	Set the timeout value, from 1 to 900 seconds, to determine the maximum time allowed to process a job before it's aborted. When an Exchange-RT Knowledge Script job runs, a job timer is started. If the transaction takes longer than the Job timeout, the transaction is stopped and a “Job Timeout" event is raised. The default is 120 seconds.
Queue timeout	Set the timeout value, from 1 to 1200 seconds, to determine how long a job can wait for resources before it's aborted. Multiple simultaneous Exchange-RT Knowledge Script jobs must wait for a token to run. If no token is available for a job you're trying to run, the job is added to the queue and starts a queue timer. When the Queue Timeout for a job expires, the job does not run, a "Queue Timeout" event is raised, and the job is moved to the end of the queue. The default is 300 seconds.

Report_Exchange-RT

Use this Report Knowledge Script to generate a report detailing availability and response time for the following Exchange-RT Knowledge Scripts:

- CheckAddressBookEntry
- OpenFolder
- OpenFolderAndRead
- SendAndReceiveMessage
- SendAndTrackMessage

Resource Object

AppManager repository

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
KS for report	Select the Knowledge Script to report on. Click the **Browse [...]** button to show the Select a Knowledge Script dialog box. Highlight an Exchange-RT script from the **Knowledge Script Name** list and click **Finish** to select it.
Exchange-RT client(s)	Select the Exchange-RT client(s). Click the **Browse [...]** button to show the **Select View(s) and a filter** dialog. From the View(s) list, select from one to twenty-five views. Your subsequent selections are limited to computers or server groups that are visible in the selected views. Select one of the Filters options: • **View:** Includes all computers in the views you selected. • **Computer:** Select from individual computers in the views you selected. • **Server Group:** Select from server groups in the views you selected. Selecting a server group includes all computers in that group.
Exchange Server or “All”	Type the name of the Exchange server or type “All” to designate all computers as Exchange servers. Default is “All”.
Select time range	In the Select Date/Time Range dialog box, set specific start and end report information dates, which is good for historical or ad hoc reports, or a sliding range (the default) that sets the time range of data to include in the report. This option is useful for reports running on a regular schedule and is the default.
Select peak weekday(s)	In the Select Peak Weekday(s) dialog box, press **Shift** to select a contiguous day range, or **Ctrl** to select non-contiguous days.

Description	How to Set It
Aggregation by	Select the time unit by which to aggregate data. The default is Hour. This works in conjunction with the next field **Aggregation interval**, which determines the number of units for one interval of data aggregation.
Aggregation interval	Select the interval units in which to aggregate data. The default is 1. For example, if you aggregate by the Hour and select 1 here, data is aggregated once every hour.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter card?	Specify whether to display a table of parameter settings in the report.
Include Availability detail table?	Specify whether to display the Availability detail table as part of the report. By default, the table is included.
Availability data stream format	Specify the data stream format. Options are 0-100 or 0-1. The default format is 0-100.
Include Availability chart?	Specify whether to display the Availability chart as part of the report. By default, the chart is included.
Threshold on Availability chart	Enter an integer for the percent. Default is 0, which means no threshold is displayed.
Include Response Time detail table?	Specify whether to display the Response Time detail table as part of the report. By default, the table is included.
Include Response Time chart?	Specify whether to display the Response Time chart as part of the report. By default, the chart is included.
Units for Response Time report	Select the response time unit of msec (the default) or sec.
Threshold on Response Time chart (selected units)	Enter the units in seconds > 0, or use the default of 0.0. Zero suppresses the threshold indicator in the chart.
Select chart style	Options in the Chart Settings dialog box set the appearance of the chart. The same parameters are used in both the availability and response time charts, if both are produced. Default is Ribbon.
Select output folder	In the Specify report folder/filename dialog box, enter an output filename and fill in the remote folder fields.
Add job ID to output folder name?	Specify whether to add a job ID to the output folder name.
Index-Report Title	In the Report Properties dialog box, configure report title settings.
Add time stamp to title	Specify whether to add a time stamp to the report title.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Generate event on success?	Specify whether an event is raised when a report is generated. By default, an event is raised.
Severity level for report success	Set the severity level for a successful report. Default is 35.
Severity level for report with no data	Set the severity level for a report with no data. Default is 25.
Severity level for report failure	Set the severity level for a report with no data. Default is 5.

Chapter 37
General Knowledge Scripts

The General category provides Knowledge Scripts for generalized monitoring tasks that can be applied to almost any application.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ADAuthentication	Monitors login time and the time required to read a property value of an object on an Active Directory server.
AsciiLog	Monitors ASCII text files for specific strings and messages logged since the last monitoring interval.
AsciiLogRX	Monitors an ASCII text file for specific strings and messages, as defined by regular expressions, logged since the last monitoring interval.
ConfigMachineDown	Loads computer-specific parameters to a local monitored computer so the MachineDownLR script, running on a group, can get the parameters required for each computer where it runs.
Counter	Monitors any System Monitor performance counter.
CounterCorrelate	Monitors thresholds for any pair of System Monitor performance counters.
EventLog	Monitors and filters information in the Windows event logs based on criteria you define.
EventLogRX	Monitors the Windows event logs for new entries matching the filter criteria you define using regular expressions.
MachineDown	Checks whether the target machine you run the script on can communicate with one or more specified Windows computers.
MachineDownLR	Using parameters planted locally by the ConfigMachineDown Knowledge Script, runs on a group of computers to check whether each computer can communicate with one or more specified Windows computers.
MissingEvent	Determines whether a Windows event log does not contain an entry matching your search criteria.
PingMachine	Checks the availability of any computers that reply to ICMP Echo requests (ping command).
Report_MachineAvailability	Generates a report about the availability of computers.
Report_PingMachine	Generates a report about the availability of computers or other machines that reply to ICMP Echo requests.
Report_ServiceChange	Generates a report about changes to the status and start-type of discovered services.

Knowledge Script	What It Does
Report_ServiceDown	Generates a report about the up/down status of discovered services.
Report_ServiceHung	Generates a report about discovered services in the Start-Pending, Stop-Pending, Continue-Pending, or Pause-Pending state.
ServiceChange	Detects any changes to the status and start type of a discovered service.
ServiceDown	Determines whether a discovered service is running.
ServiceHung	Determines whether a discovered service is hung.
ShortEventLog	Monitors and filters information in the Windows event logs based on criteria you specify.
SNMPGet	Monitors SNMP activity and allows you to check SNMP MIB variable values.
WMICounter	Monitors any WMI object property.

Creating Filters with Regular Expressions

Some Knowledge Scripts enable you to use regular expressions to define include and exclude filters for pattern-matching against the text being evaluated. Depending on the Knowledge Script you are working with, you may be able to use regular expression include and exclude filters when you are setting job properties or you may be able to maintain your search criteria independent of the Knowledge Script parameters in a separate filter file. You may also be able to use regular expression modifiers to further refine your filtering.

For example, if your **include filter** is `replic.*` and you specify the modifier `i` to make the search case-insensitive, the regular expression contains the wildcard (`.`) and repeat (`*`) special characters, indicating you want to find strings that start with `replic` followed by any string of characters. Messages containing either `replication` or `replicated` are captured.

The format is the same for the exclude filter. For example, to find log entries that do not start with the string `success`, the exclude filter might look like this:

```
^success.*
```

If you are only searching for included strings, you can leave the exclude filter blank. If you want to retrieve all messages in the log in a given interval, you can specify `.*` for the include filter and leave the exclude filter blank.

Using Special Characters

The following special characters can be used in regular expressions:

Use This Character	For This Purpose
.	Wildcard for any one character
*	Repeat zero or more occurrences
^	Beginning of the line
\$	End of the line
\	Escape the next meta-character
|	Alternate matches
[ ]	Any character in the class set. You can specify individual characters or ranges.
( )	Grouping characters. For example, you can specify (a|b|c) to indicate a match with a, or b, or c.
+	Quantifier indicating one or more occurrences
?	Quantifier indicating zero or one occurrence
{*n*}	Quantifier indicating exactly *n* occurrence
\w	A word character (alphanumeric plus _)
\s	A white-space character
\d	A digit character

Using Regular Expression Modifiers

In addition to the special characters you can use in creating the regular expression, there are a number of modifiers that can be used to modify how pattern-matching is handled. Valid modifiers include:

Modifier	Description
c	Complements the search list
g	Matches globally as many times as possible
i	Makes the search case-insensitive
m	Treats the string as multiple lines
o	Interpolates variables only once
s	Treats the regular expression string as a single long line
x	Allows for regular expression extensions

For additional information about writing regular expressions, see your Perl documentation or other regular expression resources.

ADAuthentication

Use this Knowledge Script to monitor how long it takes AppManager to log in to an Active Directory domain. You can also use this script to monitor how long it takes (response time) to read a property value of an object on the Domain Controller. This script raises an event if the login time or response read time exceeds the threshold you specify.

You can specify the Domain Controller to which you want to log in. If you do not specify a Domain Controller, then the script uses the nearest one. You must specify the account name and password used to connect to the Domain Controller.

To monitor response time for read operations, specify the LDAP path and the property name of an Active Directory object.

Resource Object

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Once every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if login or read response time exceeds threshold?	Select **Yes** to raise an event if the authentication time or response time exceeds the threshold you specify. The default is Yes.
Collect data for login or read response time?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the authentication time (in ms) and the response time (in ms). The default is unselected.
Authenticate against domain controller	Specify the name of the Domain Controller for which you want to authenticate the login. If you do not specify a name, the script uses the nearest Domain Controller. The default is `server.netiq.com`.
User name	Type the user name for the account you are using to log in.
Account password	Specify the password for the account you are using to log in. The password is stored in an encrypted format. **Note** Maximum allowed password length is 32 characters.
Threshold - Maximum login time	Specify the maximum amount of time it can take to log in to the Domain Controller before an event is raised. The default is 1000 ms.
Monitor read-response time?	Select **Yes** to monitor the time (in ms) required to read the property value of an Active Directory object from a client. The default is unselected.
LDAP path to an object on the target AD server	Specify the LDAP path to the Active Directory object for which you want to measure response time. The default is `LDAP://server.netiq.com/RootDSE`.

Parameter	How to Set It
Specify a property of the AD object	Specify a property of the Active Directory object for which you want to measure response time. The default is `serverName`.
Threshold - Maximum read time	Specify the maximum amount of time it can take to read the specified property before an event is raised. The default is 1000 ms.
Event severity when login or response time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8 (red event indicator).
Event severity level when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ADAuthentication job fails. The default is 35 (magenta event indicator).

AsciiLog

Use this Knowledge Script to monitor one or more ASCII text files for specific strings and messages logged since the last monitoring interval. Use this script to specify a pattern or search string to look for in specified ASCII files and report the matching entries found in the monitoring period. The script checks for changes to the text files that match the string you enter; it does not re-scan the entire file at each interval.

In the first interval, the script reads the file and inserts a marker at the end of the file. The script does *not* search for a specified search string during the first interval. In subsequent intervals, the script checks the file for changes that match the search string you specified. The script raises an event if the number of lines matching your search criteria exceeds the threshold you set.

Note
The script reports the number of matched lines in each iteration and the detail message contains the text data. If the detail message is larger than 32KB, the data is saved in a file on the managed computer for example, `C:\program files\netiq\appmanager\bin\log`) and the detail message contains the truncated data. If you generate these log files, periodically remove the files when you are done with them.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if matches are found?	Select **Yes** to raise events if text strings or messages that match your search criteria are found. The default is Yes.
Event severity when matches are found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which matches to your search criteria are found. The default is 15 (yellow event indicator).
Raise event if no files are found?	Select **Yes** to raise an event if no ASCII files matching your search criteria are found. The default is unselected.
Event severity when no files found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no ASCII files matching your search criteria are found. The default is 10 (red event indicator).
Raise event if no matches are found?	Select **Yes** to raise an event if no text strings or messages that match your search criteria are found in the specified files. The default is unselected.
Event severity when no matches found	Set the event severity level, from 1 to 40, to indicate the importance of an event if no matches to your search criteria are found in the specified files. The default is 20 (yellow event indicator).

Parameter	How to Set It
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the AsciiLog job fails. The default is 5 (red event indicator).
Data Collection	
Collect data for matches to search criteria?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns one or more data streams for each of your search criteria. The default is unselected. For example, if you search for `logon` and `logoff`, and `logon` is found in `C:\Log01` and `C:\Log02,` but `logoff` is not found, the script will return three data streams: • Instances of logon in `C:\Log01` • Instances of logon in `C:\Log02` • Instances of logoff Each data point in a data stream contains the number of matches found for that iteration of the script.
Monitoring	
Directory to monitor	Specify the path to the directory in which you want to begin your search, or click **Browse [...]** to navigate to that directory.
Include sub-directories?	Select **Yes** to have the script search all sub-directories of the directory you specified in *Directory to monitor*. The default is unselected.
File name (can use wildcards *, ? and %)	Specify the name of the ASCII file in which you want to search. You can use wildcards to specify filenames. The default is logfile*.log. Use the `*` wildcard to match any sequence of zero or more characters. For example, `*.log` instructs the script to search all .log files. Use the ? wildcard to match any single character. For example, `Log0?` instructs the script to search for any file whose name begins with `Log0` and includes one other character). **Note** You can use multiple instances of the `*` and ? wildcards to specify filenames; for example: `*log*.log or ??log.log.` Use the % wildcard as a placeholder for the date format specified in *Date selection format*. For example, if you routinely generate a new file of the same name each day and append the filename with a date, you can use this wildcard to tell the script to always search the latest version of the file. Use this wildcard in place of the date added to the filename. For example, if your file is `Log<`*`date`*`>`, specify the filename in this parameter as `Log%`.
Date selection format	Select the date format. If you are searching files that contain a date as part of the filename, as specified in *File name (can use wildcards *, ? and %)*, you can use this parameter to select the format.
Search patterns (separate by comma)	Specify the string for which you want to search. Separate multiple string entries by commas. **Note** The strings you enter cannot contain commas, because commas are used to separate strings from one another.
Threshold - Maximum number of matching lines	Specify the maximum number of matches to your search criteria that can be found before an event is raised. The default is 0.
Enforce case-sensitive match?	Select **Yes** to enforce a case-sensitive match to your search criteria. The default is unselected. For example, if set to Yes, search criteria of `E*.log` would match `Error.log`, but not `error.log`.

Parameter	How to Set It
Require literal match?	Select **Yes** to enforce a literal match to your search criteria. The default is unselected. For example, if set to Yes, search criteria of `NetIQ AppManager` will find strings that include the entire phrase `NetIQ AppManager`, but not strings that include only `NetIQ` or `AppManager`.
Scan entire file on first iteration?	Select **Yes** to scan entire files on the first iteration of the job. If set to No, the default, the first iteration of the job places a marker at the end of a file and scans from that point on during subsequent iterations.

AsciiLogRX

Use this Knowledge Script to monitor an ASCII text file for specific strings and messages logged since the last monitoring interval. This script allows you to use regular expressions to specify a pattern or search string to search for in an ASCII file. The script reports the matching entries found in the monitoring period. The script checks for changes to the text file that match the string you enter; it does not re-scan the entire file at each interval.

For more information, see "Creating Filters with Regular Expressions" on page 2059.

In the first interval, the script reads the file and inserts a marker at the end of the file. The script does not search for a specified search string during the first interval. In subsequent intervals, the script checks the file for changes that match the search string you specified. The script raises an event if the number of lines matching your search criteria exceeds the threshold you set.

Note
This script reports the number of matched lines in each iteration and the detail message contains the text data. If the detail message is larger than 32KB, the data is saved in a file on the managed computer (for example, `C:\program files\netiq\appmanager\bin\log`) and the detail message contains the truncated data. If you generate these log files, periodically remove the files when you are done with them.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if matches are found?	Select **Yes** to raise events if text strings or messages that match your search criteria are found. The default is Yes.
Collect data for matches to search criteria?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns one or more data streams for each of your search criteria. The default is unselected. For example, if you search for `logon` and `logoff`, and `logon` is found in `C:\Log01` and `C:\Log02,` but `logoff` is not found, the script will return three data streams: • Instances of logon in `C:\Log01` • Instances of logon in `C:\Log02` • Instances of logoff Each data point in a data stream contains the number of matches found for that iteration of the script.

Parameter	How to Set It
File name (full path)	Specify the full path to the file you want to monitor. For example `C:\temp\backup.log`. Universal Naming Convention (UNC) names are also supported (`\\ENG\appdev\mylog.txt`). **Tip** You can only specify one filename for any job instance. To monitor multiple logs or files, create separate Knowledge Script jobs.
Enforce case-sensitive match?	Select **Yes** to enforce a case-sensitive match to your search criteria. The default is unselected. For example, if set to Yes, search criteria of `E*.log` would match `Error.log`, but not `error.log`.
Find pattern (regular expression)	Specify a regular expression to identify the string you want to find in the specified file. The default is a blank string, which instructs the script to find all new strings entered since the last time the script ran.
Threshold - Maximum number of matching lines	Specify the maximum number of matches to your search criteria that can be found before an event is raised. The default is 0.
Event severity when matches are found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which matches to your search criteria are found. The default is 5.

ConfigMachineDown

Use this Knowledge Script to set parameter values in the local repository of the computer on which you run it. The values are used by the MachineDownLR Knowledge Script when it runs on that computer. Using this pair of scripts, you can set up individual computers in a group so that when MachineDownLR runs on the group, it can run with different parameter values on each computer. This is particularly useful for enforcing monitoring policies.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if parameter values set successfully?	Set to **y** to raise an event if the script successfully sets parameter values in the local repository. The default is y.
List of computers separated by commas (no spaces)	Specify all the computers you want this computer to monitor when MachineDownLR runs on it.
Full path to file with a list of computers (one per line, no commas or spaces)	Specify the path and filename of a text file containing a list of computers for this computer to monitor when MachineDownLR runs on it. The file must be a text file with the name of each computer on a separate line (no spaces).
Event severity when parameter values set successfully	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this script successfully sets parameter values in the local repository. The default is 25 (blue event indicator).

Counter

Use this Knowledge Script to monitor System Monitor performance counters. You can run this script on any computer or server to monitor any counter available in System Monitor. You can configure the script to raise an event if the value of the counter you select exceeds or falls below the threshold you set. You can also specify a consecutive number of times that a threshold must be exceeded before an event is raised.

Use this Knowledge Script to yield performance information for the counters you want to monitor. When this script collects and graphs data, the results are similar to the results displayed in System Monitor. Use the counter data to start corrective actions when thresholds are exceeded, generate more complex and sophisticated graphs, and provide historical information for reporting, trend analysis, and capacity planning.

Prerequisites

Requirements for **Windows Server 2003**:

- The Log On As account under which the management agent runs on Windows Server 2003 must belong to the Performance Monitor Users policy.
- If the Operator Console or Control Center is installed on Windows Server 2003, the user account under which the console application runs must belong to the Performance Monitor Users policy.

  To check the local policy:

  1. At a Command Prompt, type `gpedit.msc` and press `Enter`.

  2. In the Group Policy snap-in, double-click **Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.

  3. In the **Local Setting** column, ensure the appropriate user account belongs to the **Performance Monitor Users** policy.
- If the Operator Console or Control Center is installed on Windows Server 2003, the Remote Registry service on the console computer must be running. If the Remote Registry service is down when you attempt to configure this script by browsing counter information on the remote computer, the console displays an error message that indicates AppManager was unable to connect to the remote computer.

Requirements for **Windows Vista**:

If the Operator Console or Control Center is installed on Windows Vista, the Remote Registry service on the console computer must be running. If the Remote Registry service is down when you attempt to configure this script by browsing counter information on the remote computer, the console becomes unresponsive.

Resource Object

Windows computer or application server, such as Exchange Server or SQL Server

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Counter job fails. The default is 5.
Event severity when no counter or instance is found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the script cannot find the counter or instance you specified. The default is 15 (yellow event indicator).
Raise event when counter value exceeds threshold?	Select **Yes** to raise an event if the counter value exceeds the threshold *n* consecutive times. Specify the value of *n* in the *Consecutive times threshold can be crossed before event is raised* parameter. The default is Yes.
Event severity when counter value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a value exceeds the threshold you set. The default is 8 (red event indicator).
Threshold - Maximum counter value	Specify the highest value a counter can attain before an event is raised. The default is 600.
Raise event when counter value falls below threshold?	Select **Yes** to raise an event if the counter value falls below the threshold *n* consecutive times. Specify the value of *n* in the *Consecutive times threshold can be crossed before event is raised* parameter. The default is Yes.
Event severity when counter value falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a value falls below the threshold you set. The default is 8 (red event indicator).
Threshold - Minimum counter value	Specify the lowest value a counter must maintain to prevent an event from being raised. The default is 20.
Monitoring	

Name of counter to monitor	Provide the name of the object/counter/instance you want to monitor, or click **Browse [...]** to select the computer and counter you want to monitor. You can also select a counter to monitor by starting System Monitor and clicking **Add** [**+**] in the toolbar. The default is `Objects\Threads\`.
	If typing the name, use the format <*`object`*>\<*`counter`*>\<*`instance`*>. You can enter multiple instances, separated by commas. For example:
	`Process\% Privileged Time\mapisp32,mqsvc`
	For more information, see "Examples of Using This Script" on page 2071.
	Tips
	• If an instance is a parent of multiple instances (for example, if you have a Logical Disk 0 with partitions C: and D:), enter the complete instance name exactly as displayed in System Monitor. For example: `0 ==> C:`
	• To monitor multiple instances of the same instance name, use one of the following methods:
	  • Indicate the instance index in parentheses to monitor specific instances. For example:
	  `Process\% Privileged Time\netiq,netiq(1),netiq(2)`
	  • Use an asterisk (*) after the instance name to monitor all instances that begin with the string you provide. For example:
	  `Process\% Privileged Time\netiq*`
	  • Use an asterisk (*) before the instance name to monitor all instances that end with the string you provide. For example:
	  `Process\% Privileged Time\*netiq`

Parameter	How to Set It
Consecutive times threshold can be crossed before event is raised	Specify the number of consecutive times a counter value can exceed or fall below the threshold before an event is raised. The default is 1 time. **Tip** This parameter provides functionality similar to that of the *Raise event if event condition occurs x times within y job iterations* parameter on the Advanced tab. NetIQ recommends using the *Consecutive times threshold ...* parameter when you run this script. The *Consecutive times threshold ...* parameter is designed to match the event text that is particular to this script, which can vary depending on your entry for the *Name of counter to monitor* parameter. In summary, use the *Consecutive times threshold ...* parameter to raise events. Leave the *Raise event if event condition ...* parameter at the default setting of **1** time within **1** job iteration.
Data Collection	
Collect data for counter value?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns values for counters that exceed the threshold. The default is unselected.

Examples of Using This Script

The following are examples of providing information in the *Name of counter to monitor* parameter.

Simple Counter with No Instance Name

For example, to monitor the Cache Hit Ratio counter and create one data stream, set the *Name of counter to monitor* parameter as follows:

```
SQLServer\Cache Hit Ratio
```

For this type of counter you can simply leave the instance parameters blank. If selecting this counter through the Counter Browser:

1. Click **Browse [...]** and select the target **Computer**.
2. Select **SQLServer** from the Object list.
3. Select **Cache Hit Ratio** from the Counter list and click **OK**.

Counter with Multiple Identical Instance Names

Assume you want to monitor the percentage of processor time used by several `cmd` processes running on a given computer. If you enter `cmd` as the instance name, only the first `cmd` process found is monitored.

To monitor additional `cmd` processes, or to select a specific `cmd` process rather than the "first found," you need to specify the instance index. The simplest way to select multiple instances is through the Counter Browser.

The script will monitor the processor time for these three `cmd` processes and create three data streams.

If you do not use the Counter Browser and there are multiple instances with the same name, you need to identify which instance to monitor using an instance index, with 0 indicating the first instance, 1 the second, and so on. If you do not enter an index, the first instance found is monitored. If you are typing the information in the *Name of counter to monitor* parameter, use the format `<object>\<counter>\<instance> (<instance_index>)`. For example:

```
Process\% Privileged Time\cmd (0),cmd (1),cmd (3)
```

Counter with Parent-Child Instances

In some cases, an instance is a **parent** of multiple **child** instances. For example, if you have a Logical Disk `0` with partitions `C:` and `D:`, the logical disk `0` is the parent of the logical disk `C:` and the logical disk `D:`. In addition, there may be multiple child instances with identical names. For example, two processes called `MSDEV` may each have threads 0, 1, 2, and 3:

```
Instance    ProcessID  ThreadID Instance Index
-------------------------------------------
MSDEV ==> 0    361        495      0
MSDEV ==> 0    291        426      1
MSDEV ==> 1    361        275      0
MSDEV ==> 1    291        181      1
MSDEV ==> 2    361        471      0
MSDEV ==> 2    291        256      1
MSDEV ==> 3    361        376      0
MSDEV ==> 3    291        500      1
```

The simplest way to select these child instances is through the Counter Browser. If you do not use the Counter Browser and there are child instances, you need to identify which instance to monitor using the format `<object>\<counter>\<parent_instance> ==> <child_instance>`. For example:

```
LogicalDisk\% Free Space\0 ==> C:
```

If there are multiple child instances with the same name, you need to identify which child instances to monitor using an instance index, with 0 indicating the first instance, 1 the second, and so on. If you do not enter an index, the first instance found is monitored.

If you are typing the Counter to monitor, use the format: `<object>\<counter>\<parent> ==> <child> (<index>)`. For example:

```
Thread\% Processor Time\MSDEV ==> 0 (0),MSDEV ==> 0 (1)
```

Using the example above, this counter would get `% Processor Time` for threads 495 (`MSDEV` process 361) and 426 (`MSDEV` process 291) and create two data streams.

```
ID  Job KS Name          Legend
-------------------------------------------------------------
7   12  General_Counter  Thread-% Processor Time-MSDEV ==> 0(0)
6   12  General_Counter  Thread-% Processor Time-MSDEV ==> 0(1)
```

Format for Entering Counter Names without Browsing

To type counter names rather than use the Counter Browser, enter the complete instance name exactly as it is displayed in the Performance Monitor, including any spaces or spelling conventions.

To manually set the *Name of counter to monitor* parameter (without browsing), use one of the following formats:

Counter Type	General Format to Use and Example
Single counter instance	<object>\<counter>\<instance_name>`Process\% Privileged Time\cmd`
Multiple instances	<object>\<counter>\<instance> (<instance_index>)`Process\% Privileged Time\cmd (1),cmd (4)`
Child instances	<object>\<counter>\<parent_instance> ==> <child_instance>`LogicalDisk\% Free Space\0 ==> C:`
Multiple child instances	<object>\<counter>\<parent> ==> <child> (instance_index)`Thread\% Processor Time\MSDEV ==> 0 (0),MSDEV ==> 0 (1)`

CounterCorrelate

Use this Knowledge Script to monitor any pair of System Monitor performance counters. You can run this script on any computer or server, and you can monitor any counters available in the System Monitor. You can observe either a maximum or minimum threshold for each counter you are monitoring. You can set the script to raise an event if the value of either counter exceeds or falls below the threshold you set.

To see a list of available counters, click **Browse [...]** in the *Name of counter to monitor* parameter or start the System Monitor and click **Add [+]** in the toolbar.

If the Operator Console or Control Center is installed on **Windows Server 2003**, the Remote Registry service on the console computer must be running. If the Remote Registry service is down when you attempt to configure this script by browsing counter information on the remote computer, the console displays an error message that indicates AppManager was unable to connect to the remote computer.

If the Operator Console or Control Center is installed on **Windows Vista**, the Remote Registry service on the console computer must be running. If the Remote Registry service is down when you attempt to configure this script by browsing counter information on the remote computer, the console becomes unresponsive.

Use this Knowledge Script to monitor for conditions when the values for any pair of counters indicate a problem. For example, you can raise events when CPU and memory counters both exceed a high threshold, or when a data file size counter exceeds a high threshold and an available disk space counter falls below a low threshold.

Resource Objects

Windows computer or application server, such as Exchange Server, SQL Server, IIS server

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data for counter value?	Set to **y** to collect data for charts and reports. If enabled, data collection returns values for counters that exceed the threshold. The default is n.
Raise event if counter value exceeds or falls below threshold?	Select **yes** to raise an event when a counter value counter exceeds or falls below the threshold you set. The default is yes.
Counter 1 Settings	
Counter value for threshold	Specify the value for the threshold you want to observe. The default is 600.
Use counter value as maximum threshold?	Select **yes** to use the value from the *Counter value for threshold* parameter as a maximum threshold. The script then raises events when the counter value exceeds the threshold. Deselect the yes check box to use the value from the *Counter value for threshold* parameter as a minimum threshold. The script then raises events when the counter value falls below the threshold. The default is yes.

Parameter	How to Set It
Name of counter to monitor	Specify the object\counter\instance name or click **Browse [...]** to select the object, counter, and instances to monitor. If typing the name, use the format `<object>\<counter>\<instance>`. You can enter multiple instances, separated by commas. For example: `Process\% Privileged Time\mapisp32,mqsvc` If an instance is a parent of multiple instances (for example, if you have a Logical Disk 0 with partitions C: and D:), enter the complete instance name exactly as displayed in Performance Monitor (for example "`0 ==> C:`"). For more information, see "Examples of Using This Script" on page 2071.
Counter 2 Settings	
Counter value for threshold	Specify the value for the threshold you want to observe. The default is 600.
Use counter value as maximum threshold?	Select **yes** to use the value from the *Counter value for threshold* parameter as a maximum threshold. The script then raises events when the counter value exceeds the threshold. Deselect the yes check box to use the value from the *Counter value for threshold* parameter as a minimum threshold. The script then raises events when the counter value falls below the threshold. The default is yes.
Name of counter to monitor	Specify the object\counter\instance name or click **Browse [...]** to select the object, counter, and instances to monitor. If typing the name, use the format `<object>\<counter>\<instance>`. You can enter multiple instances, separated by commas. For example: `Process\% Privileged Time\mapisp32,mqsvc` If an instance is a parent of multiple instances (for example, if you have a Logical Disk 0 with partitions C: and D:), enter the complete instance name exactly as displayed in the Performance Monitor (for example "`0 ==> C:`"). See System Monitor for the exact spelling of counter names and details about what each counter represents.
Event severity when counter value exceeds or falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event if a counter value exceeds or falls below the threshold you set. The default is 8 (red event indicator).

EventLog

Use this Knowledge Script to monitor and filter information in Windows Event Logs. With this script, you can track Windows event log entries that match filtering criteria. This script works on an incremental basis; it does not fully rescan the event log each time it runs. This script returns all event log entries that match the filtering criteria in the event or data point detail message.

Notes

- Only the most recent batch of events can be viewed in the data point detail message. For example, assume you set this script to scan all previous entries in the event log and list ten matching entries in each event detail message and when the job runs, 30 entries are found that match your filtering criteria. In this case, the job creates three child events for the interval, and each child event contains ten entries: the oldest matching entries in one child event batch, the second oldest in Batch 2, and the most recent in Batch 3. If this same job is collecting data and you view the data detail message for the interval, only the entries from the third child event (Batch 3) are displayed.
- When you use text/numeric strings in the *Event [...] filter* parameters, this script searches event logs and matches the text/numeric string to any part of the event entry. The results are not exact matches. For example, if your filter string is "foo," results will include "foobar," "foo," and "food."

Resource Objects

Windows computer or application server, such as Exchange Server or SQL Server

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the EventLog job fails. The default is 5.
Event Log Monitoring	
Event logs to monitor	Provide a comma-separated list of the event logs you want to monitor. For example: `System,Application,Security` The default is `Application`. **Note** If the event log you specify does not exist on the target computer, the Application log is automatically monitored.

Parameter	How to Set It
Number of previous hours to scan logs	Set this parameter to control how the script scans the logs at the first interval, after which scanning begins where the previous scan ended. Enter one of the following values: • **-1** -- to scan all the existing entries • ***N*** -- to scan entries only for the past *n* hours (8 for the past 8 hours, 50 for the past 50 hours, for example) • **0** -- to not scan previous entries; only search from this moment on. The default is 0.
Maximum number of entries per event report	Specify the maximum number of entries to be recorded in each event's detail message. If this script finds more entries from the log than can be put into one event message, it will return multiple events to report all the outstanding entries in the log. The default is 30 entries. If this script encounters one or more very large events in the Windows Event log, this script may error out and generate an event message "`Out of string space`." If this occurs, you can usually work around the problem by adjusting this parameter to a smaller value.
Event Log Filters	
Event Types	
Monitor error events?	Select **Yes** to monitor error event entries. The default is Yes.
Monitor warning events?	Select **Yes** to monitor warning event entries. The default is Yes.
Monitor information events?	Select **Yes** to monitor information event entries. The default is Yes.
Monitor success audits?	Select **Yes** to monitor success audit event entries. Success audits are successful security access attempts that are audited. The default is Yes.
Monitor failure audits?	Select **Yes** to monitor failure audit event entries. Failure audits are failed security access attempts that are audited. The default is Yes.
Monitor unclassified events?	Some events written to Windows event logs do not have event levels or severities set to event types recognized by Windows Server 2008 and later. This Knowledge Script identifies these entries as unclassified. These entries will not be found by the error, warning, information, success audit, or failure audit filter criteria. Select **Yes** to monitor log entries that are unclassified. The default is Yes.
Event source filter	To filter for events generated by a particular source (such as SQLExecutive, SNMP, or the Service Control Manager), enter a search string. This script will look for matching entries in the Event Log's **Source** field. Separate multiple strings with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.
Event category filter	To filter for events in a particular category (such as Server or Logon), enter a search string. This script will look for matching entries in the Event Log's **Category** field. Separate multiple strings with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.

Parameter	How to Set It
Event ID filter	To filter for particular event IDs, enter a search string or ID range (for example 100-2000). This script will look for matching entries in the Event Log's **Event** field. Separate multiple IDs and ranges with commas. For example: `1,2,10-15,202`. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.
Event user filter	To filter for events associated with a particular user, enter a search string, for example, `<domain name>\<user name>`. This script will look for matching entries in the Event Log's **User** field. Separate multiple strings with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary
Computer filter	To filter for events generated by a particular computer, enter a search string. This script will look for matching entries in the Event Log's **Computer** field. Separate multiple strings with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.
Event description filter	To filter for events with a particular detail description or containing keywords in the description, enter a search string. This script will look for matching entries in the Event Log's **Description** field. Separate multiple strings with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary
Event Notification	
Raise event if log entries matching criteria are found?	Select **Yes** to raise an event when log entries match your filtering criteria. The default is Yes.
Event severity when log entries match criteria	Set the event severity level, from 1 to 40, to indicate the importance of an event in which log entries match your search criteria. The default is 15 (red event indicator). **Tip** You can adjust the severity based on which log or type of event you are checking for.
Data Collection	
Collect data for log entries that match criteria?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns detail about log entries that match your filtering criteria. The default is unselected.
Separate data by log file type?	Select **Yes** to separate event entries from different log files into different data streams. If unselected, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. For example, if you are monitoring both the System and Application logs, you can enable this parameter so that events in the System log are tracked separately from events in the Application log. The default is unselected.

Examples of How this Script Is Used

You can customize this script in many ways based on your requirements. For example, for general system events, you can set the following options when detecting security failures:

Properties and Parameters	How You Might Set Them
Schedule interval	10 minutes
Raise event if log entries match criteria?	Yes
Log files to filter	Security
Monitor failure audits?	Yes
Event severity when event log entries match criteria	2
Action	MapiMail

With this scenario, on the **Schedule** tab in the Knowledge Script Properties dialog box, set the interval to **Once very 10 minutes** because you want a short window for checking for this type of problem.

On the **Values** tab, enable the *Raise event if log entries match criteria?* parameter, indicate you will monitor failure audits in the Security log, and set the event severity to 2, indicating this is a very serious event that should be highly visible. Leave the other filtering options blank.

On the **Action** tab, indicate that you want an e-mail sent if an event is raised. With these settings, AppManager for Microsoft Windows will regularly check for security failures and will notify you, or whoever you designate, through e-mail if any security failure events are detected.

Another example of how to use this script to detect all problems with your SQL Server could involve setting up the script job like this:

Properties and Parameters	How You Might Set Them
Schedule interval	30 minutes
Raise event if log entries match criteria?	Yes
Log files to filter	Application
Monitor error events?	Yes
Event source filter	MSSQLServer
Event severity when event log entries match criteria	8
Action	MapiMail

Another way you can use this script is to collect data and graph a trend chart from your System event log:

Properties and Parameters	How You Might Set Them
Schedule interval	1 hour
Collect data for log entries that match criteria?	Yes
Log files to filter	System
All other filters	not set
Action	Null

If you choose to collect data, the script returns the number of matched entries as the primary data point to be graphed. The first batch of filtered results can be viewed in the detail data message when you double-click a data point. Additional matching entries may be included in the graph. The peaks and valleys in the graph indicate a large number of events or low event activity.

EventLogRX

Use this Knowledge Script to scan the Windows logs you specify for entries that match the criteria you specify. You can filter the event log entries by event type and by specifying a combination of include and exclude strings for each event field using regular expressions. This script raises an event if a log entry matches all the filter criteria you specify. All event log entries that match the filtering criteria are returned in the event detail message.

Use the *Filter the [...] field with the regular expression* parameters to control which fields to filter and the filtering criteria to use to find specific information, such as events associated with a specific user or computer name. With this script, you specify the filtering criteria for each field you are interested in using a regular expression or you can specify the name of a file that contains all your filtering criteria.

For more information, see "Creating Filters with Regular Expressions" on page 2059.

You can use the *Events in past N hours* parameter to determine the number of previously recorded event entries, if any, to scan for matches. For example, if you want to check whether any event entries recorded in the last two hours match your filtering criteria, you would set this parameter to 2. To scan the entire log for any previously reported events, set the *Events in past N hours* parameter to 1. After the Knowledge Script job completes its first iteration, only new entries written to the event log that match your criteria are reported. When the *Events in past N hours* parameter is set to 0, the script does not scan the log for any previously reported events.

Prerequisite

This script requires the Async managed object to be installed and the Microsoft EventLog service to be running on the computer you want to monitor.

Resource Objects

Windows computer or application server, such as Exchange Server or SQL Server

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the EventLogRX job fails. The default is 5.
Event Log Monitoring	

Parameter	How to Set It
Log files to filter	Specify the event log you want to monitor. You can specify multiple event logs, separated by commas. For example: `System,Application,Security`. The default is `Application`. If you do not specify an event log, AppManager monitors all logs. **Notes** • If, in addition to these event logs, you specify a filter file in the *Full path to a file containing filtering criteria* parameter, AppManager ignores the *Filter the [...] field with the regular expression* parameters, but continues to scan the log file you specified. • If the event log you specify does not exist on the target computer, the Application log is automatically monitored.
Number of previous hours to scan logs	Set this parameter to control how the script scans the logs at the first interval, after which scanning begins where the previous scan ended. Enter one of the following values: • **-1** -- to scan all the existing entries • ***N*** -- to scan entries only for the past *n* hours (8 for the past 8 hours, 50 for the past 50 hours, for example) • **0** -- to not scan previous entries; only search from this moment on. The default is 0.
Enforce case-sensitive filters?	Select **Yes to** make all filter statements for this script case-sensitive. The default is unselected.
Maximum number of entries per event report	Specify the maximum number of entries to be recorded in each event's detail message. If this script finds more entries from the log than can be put into one event message, it will return multiple events to report all the outstanding entries in the log. The default is 30 entries. If this script encounters one or more very large events in the Windows Event log, this script may error out and generate an event message "`Out of string space`." If this occurs, you can usually work around the problem by adjusting this parameter to a smaller value.
Full path to a file containing filtering criteria	Type the full path to a file containing the filtering criteria you want to match if you want to specify matching expressions in an external file. For example: `C:\TEMP\MyFilters.txt`. **Note** If you specify a filter file, AppManager ignores the *Filter the [...] field with the regular expression* parameters, but continues to scan the log file specified in the *Log files to filter (Application, Security, System)* parameter. However, if AppManager cannot process the filter file, the script raises an event (for example, `fail to process filter file C:\general.xml`) and continues to scan the log file using the filtering criteria you specified in the *Filter the [...] field with the regular expression* parameters.

Event Log Filters

Parameter	How to Set It
Filter the [...] field with a regular expression	Use a regular expression to specify the criteria to look for in each event log field you want to monitor: • **Type**. To filter information based on the type of event (for example, Error, Warning, Information, Audit_Success, Audit_Failure), use a regular expression to identify the type of event entries to include. • **Source**. To filter the entries generated by a particular source (for example `SQLExecutive`, `SNMP`, or `Service Control Manager`), use a regular expression to identify the source of event entries to include. • **Category**. To filter information based on a particular category (for example Server or Logon), use a regular expression to identify the category of event entries to include. • **Event ID**. To filter information based on the event ID, use a regular expression to identify the event IDs to include. • **User**. To filter information based on the user name, use a regular expression to identify the user names to include. • **Computer**. To filter information based on the computer name, use a regular expression to identify the computers to include. • **Description**. To filter information based on the event description, use a regular expression to indicate the description to include. **Note** If you specify a filter file in the *Full path to a file containing filtering criteria* parameter, AppManager ignores the *Filter the [...] field with the regular expression* parameters, but continues to scan the log file specified in the *Log files to filter (Application, Security, System)* parameter.
Event Notification	
Raise event if log entries matching criteria are found?	Select **Yes** raise an event when log entries match your filtering criteria. The default is Yes.
Event severity when log entries match criteria	Set the event severity level, from 1 to 40, to indicate the importance of an event in which log entries match your search criteria. The default is 15 (red event indicator). **Tip** You can adjust the severity based on which log or type of event you are checking for.
Data Collection	
Collect data for log entries that match criteria?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns detail about log entries that match your filtering criteria. The default is unselected.
Separate data by log file type?	Select Yes to separate event entries from different log files into different data streams. If unselected, all event entries matching your filtering criteria are placed in the same data stream and the data detail message can include event entries from multiple log sources. The default is unselected. For example, if you are monitoring both the System and Application logs, you can enable this parameter to track events in the System log separately from events in the Application log.

Examples of How this Script Is Used

Using this script you can specify regular expressions for each event log field as Knowledge Script properties or maintain your search criteria independent of the Knowledge Script parameters in a separate filter file.

In many cases, specifying an external filter file provides greater flexibility and makes modifying your search criteria more straightforward because you can add almost any number of expressions and you do not need to modify the Knowledge Script properties to pick up your changes.

If you want to use a filter file:

- Identify the strings that you want to find a match for (that is, the entries you want to include in your results).
- Create a text file with one regular expression string per line to locate matching strings. Each line in the file consists of a parameter keyword followed by a colon (:), a tab or blank space, and the regular expression. Or the filter file can be written using XML.
- Make sure the file exists on the target computer.
- Type the absolute path to the file on the local computer in the *Full path to a file containing filtering criteria* parameter and start the job.

Formatting the Filter File

There are two valid formats for the filter file: a simple table format to define the strings to include and an XML format that allows you to define more complex include and exclude filtering. For both formats, the parameter name keywords are required, but the field values can be left blank if no filtering is needed.

Select a file format appropriate for the complexity of the filtering you need to do.

Table Format

The table format provides a simple way to create the filter file. Each filtering section in the file begins with `EventStart` and ends with `EventEnd`. If an entry in the event log matches all the criteria you have specified within a filtering section, it is considered a match and an AppManager event is raised. If you have more than one filtering section, an entry matching either section raises an event.

For example, the following table format file provides two filter sections:

```
EventStart
CaseSensitive:n
Log:System
Type:Error|Warning|Information
Source:^SQL*
Category:*
EventID:1[0-9][0-9][0-9]
User:Sam|Joe|Chris
Computer:SFO*
Description:($Error.*)|(.*error.*occurred.$)
EventEnd
EventStart
CaseSensitive:n
Log:Application
Type:Error|Warning|Information
Source:^SQL*
Category:*
EventID:1[0-9][0-9][0-9]
User:Sam|Joe|Chris
Computer:SFO*
Description:($Error.*)|(.*error.*occurred.$)
EventEnd
```

Note

If you are only specifying one filter section, you do not need to include the EventStart and EventEnd lines in the file. These lines are only required if you have more than one filtering section.

XML Format

The XML format is somewhat more sophisticated and more flexible than the table format. The XML format allows you to set both include and exclude filters using the `<Include>` and `<Exclude>` tags and to combine these filter sets to define the search criteria. Each filtering section in the file begins with the `<Events>` tag. A log entry must match all the criteria you specified within a filtering section for it to be considered a match.

For example:

```
<?xml version = "1.0" standalone = "yes"?>
<EventLogConfig Name = "Event Filter" Type = "EVENT_FILTER_CUSTOM" ID = "76">
<Include>
   <Events>
      <Log>Application</Log>
      <Type>INFORMATION|WARNING|ERROR</Type>
      <Source><Net*]></Source>
      <Category>*</Category>
      <EVENTID>2*</EVENTID>
      <User>*</User>
      <Computer>*</Computer>
      <Description><![CDATA[Event.]]></Description>
      <CaseSensitive>y</CaseSensitive>
   </Events>
   <Events>
      <Log>System</Log>
      <Type>Warning</Type>
      <Source>RSVP</Source>
      <Category>*</Category>
      <EVENTID>*</EVENTID>
      <User>*</User>
      <Computer>SHASTA</Computer>
      <Description>RSVP*</Description>
      <CaseSensitive>y</CaseSensitive>
   </Events>
</Include>
</EventLogConfig>
```

Note

If a field contains a regular expression that conflicts with XML syntax or includes special characters, you can use `![CDATA[regular_expression]]` to enclose the expression and prevent parsing problems.

MachineDown

Use this Knowledge Script to detect whether the computer on which you run the script can communicate with one or more specified Windows computers.

This script does **not** require the AppManager agent to be installed on the remote computers you want to monitor.

To run this script on a Windows Vista computer, the Remote Registry service on the agent computer must be running to connect to the Windows registry on the remote computers you want to monitor. If the Remote Registry Service is down when this script runs, an event is raised to indicate the remote computer was unresponsive and the connection to the Windows registry failed.

You can select computers by browsing the AppManager repository, specifying a list of computers using the *Computers to monitor* parameter, or naming a file that contains a list of computer names or addresses. Browse the AppManager repository to select the remote computers you want and prevent event information from appearing in the Operator Console while the computer is in maintenance mode.

If you specify a list of computers, instead of browsing the repository for the computers you want, this script displays event information in the Operator Console even if the remote computer is in maintenance mode.

When typing a list of Windows computers, you can specify computers that are not currently in the TreeView pane of the Operator Console.

When you run this script on a computer, the script tries to communicate with each of the computers you specified in the *Computers to monitor* parameter.

This script attempts to communicate by:

- Checking name-to-IP-address resolution
- Executing an Internet Control Message Protocol (ICMP) ping
- Connecting to the Windows registry

This script raises an event if any of these attempts fail.

You can also instruct the script to ping specific router IP addresses before attempting to communicate with any of the specified computers. This provides an additional test of the network connection between the computer on which the script is running and the monitored computers. If this test is successful, it eliminates one reason for a lack of communication between computers.

This script does not monitor the computer where the script itself is running. For example, if you run this script on a server named SERVER01 and use the Select computers from the Repository parameter to select the server SERVER01 (either explicitly or as a member of a group or view), the script automatically excludes SERVER01 at run time because it does not make sense to monitor the local computer's availability. If the script is running, the computer must be available. If the script is not running, either the local computer is down or the script or agent has been stopped.

To monitor the local computer, create a second MachineDown job running on a different computer that monitors the local computer in question. In this case, you could have a server SERVER02 running the script and monitoring SERVER01 and server SERVER01 monitoring server SERVER02. If both jobs are collecting data, be careful that the two scripts are not monitoring the same computers, for example, SERVER01 and SERVER02 should not both monitor SERVERA. This would result in two data streams collecting uptime information for the same server (SERVERA), which can cause the ComputerAvailability report to miscalculate the uptime for SERVERA.

In some cases, this script may not be able to communicate with one or more remote computers because Update Definition in User Variables. does not have sufficient privileges to access those remote machines. To avoid this problem, grant Admin privileges to the Update Definition in User Variables. agent's user account or use the PingMachine Knowledge Script to check connectivity.

If you select target computers by browsing the AppManager repository, the logon account for the agent on which the job is running must have sufficient privileges to query the AppManager repository.

If you select to include computers from the AppManager repository by View or Server Group, AppManager automatically includes the new computers on the next iteration. If you select to include computers from the AppManager repository by Computer, AppManager only monitors the computers that were selected. However, if you delete a monitored computer from the AppManager repository, AppManager does not monitor that computer unless you add it back into the AppManager repository. AppManager also reads the server list file on every script iteration. If you remove a computer name from the server list file, starting with the next script iteration, AppManager no longer monitors the computer.

This script can check connections to computers that are across a firewall from the AppManager repository so long as the script is running on a computer on the same side of the firewall as the computers to which it is checking connections. Keep in mind, however, that under these circumstances you cannot select computers by browsing the AppManager repository unless the SQL Server communication ports are open in the firewall and the agent can query the AppManager repository. If you are using an agent across a firewall from the AppManager repository, you are advised to use the *Computers to monitor* or *Filename for computer list* parameter to specify computers.

If you are running version 6.0 of this script, you need to run version 6.0 of Report_MachineAvailability to create an accurate report based on the data you collect. Version 6.0 of this script works only in conjunction with AppManager repositories version 6.0 and later.

If the computer that is down has been discovered and is displayed in the TreeView, that computer's icon blinks in the TreeView. If the computer that is down is not displayed in the TreeView, the computer where you ran the Knowledge Script blinks instead.

For computers running AppManager agents version 6.x and later where you want to use a monitoring policy, consider using the ConfigMachineDown and MachineDownLR Knowledge Scripts.

When configuring an action for this Knowledge Script, configure the Location to initiate the action on the MS (to run on the management server) or on a Proxy (to run on a particular managed client).

If you instead configure an action to run on the managed client (MC), when a remotely monitored computer is placed into machine maintenance mode (from the Operator Console) or scheduled maintenance mode (using the AMAdmin_SchedMaint Knowledge Script), any event conditions detected on the remote computer are ignored, but the action is not disabled. In this case, an action runs, but no event information appears on the **Events** tab of the Operator Console.

Use the ReportAM_GeneralMachineDown Knowledge Script to generate a report about computers that were detected as down during a specified period.

If you are using the Web Console, the *Select computers from the repository* parameter is not supported. Instead, use the *Computers to monitor* parameter to specify the computers you want to monitor.

Using this Script to Monitor a Subnet

Run this script on a computer in the same subnet as the management server. When completing the *Computers to monitor* parameter, specify a limited number of computers that represent different subnets in your network.

You can then run additional MachineDown jobs on each of the computers specified in the first job to monitor the computers in each of their own subnets. This gives you coverage without stressing network bandwidth. It also ensures that, if a router or subnet is down, you receive only one event for the server being monitored from the agent on the management server's subnet. The other servers in that subnet will not post duplicate "Computer Down" events.

As an example, assume:

- The AppManager for Microsoft Windows management server is installed on the computer `TARZAN` in subnet 1. Other servers in subnet 1 include `TITO` and `BLUE`.
- Subnet 2 includes the servers `PAOLO`, `BONN`, and `KENO`.
- Subnet 3 includes the servers `TRISTE`, `VOILA`, and `TONTO`.

You create a Knowledge Script job that runs on `TITO` (subnet 1, same as the management server) and set the *Computers to monitor* parameter to `PAOLO` (subnet 2) and `TRISTE` (subnet 3).

You then create a job (J-2) on `PAOLO` with the *Machine list* parameter set to `BONN` and `KENO`, and a job (J-3) on `TRISTE` with the Machine List set to `VOILA` and `TONTO`. Also create a job that runs on the management server (for example, `TARZAN`) that does a reciprocal check with the server in its own subnet (for example, `TITO`) in its *Computers to monitor* parameter.

Tip
If you want this Knowledge Script to raise an action when a connection is down, enable the *Managed Client Action* parameter in the Knowledge Script Properties dialog box for the job that monitors your subnets.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Every 5 minutes**.

Be sure to schedule this job so that you allow enough time for the job to complete during the interval. As a general guideline, allow 20 to 30 seconds for each computer being monitored. This allows enough time for the connection to the registry on each computer.

You can use the following formula to calculate how many minutes are required for the job to complete:

```
(number of computers x 30 seconds)/60 = minutes for job to complete
```

For example:

```
(10 computers x 30 seconds)/60 = 5 minutes
```

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if a computer is down?	Select **Yes** to raise an event if a connection cannot be established to the target computer. The default is Yes. **Note** For AppManager agents version 6.x and later, events raised for computers in maintenance mode are suppressed.
Require Windows Registry connection?	Select **Yes** to require the script to attempt a connection to the registry after it has attempted an ICMP ping. The default is Yes. This test is recommended because Windows can respond to ICMP ping requests even though the computer is in a blue screen state. A connection to the registry is further validation that the target computer is up. If you are using this script to check the status of UNIX machines, you must disable this option. **Note** The account under which the AppManager agent is running must have sufficient privileges to connect to the registry.
Event severity when computer is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a connection cannot be established to the target computer. The default is 5 (red event indicator).
Raise single event for all computers that are down?	Select **Yes** to raise only one event regardless of the number of computers that are down. The default is unselected. If you choose to raise only a single event, the information about specific computers is contained in the event detail message. The same rules for the suppression of events that apply to the *Raise event if a computer is down* parameter also apply here.
Raise event if specified router is down?	Select **Yes** to raise an event if a router specified in the *Router IP addresses* parameter is down. The default is Yes.
Event severity when router is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a specified router is down. The default is 5 (red event indicator).
Raise event if default gateway is down?	Select **Yes** to raise an event when the default gateway is down. The default is Yes. If the default gateway is down, the script might not be able to connect to any of the computers you identified, and false events can be raised,
Event severity when default gateway is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the default gateway is down. The default is 5 (red event indicator).
Raise event if the computer list file is missing?	Select **Yes** to raise an event if the file containing the list of monitored computers cannot be found. The default is Yes.
Event severity when computer list file is missing	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the list of monitored computers cannot be found. The default is 15 (yellow event indicator).
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MachineDown job fails. The default is 5 (red event indicator).
Data Collection	

Parameter	How to Set It
Collect data for each monitored server?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the availability, or status, of a specific computer you are monitoring. The default is unselected.
Collect single data point for number of servers down?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of unavailable, or down, computers for the monitored machines. The default is unselected.
Collect data for default gateway availability?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the availability, or status, of the default gateway of the computer that is running the job. The default is unselected.
Collect data for router availability?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the availability, or status, of one or more routers that you configured in the *Router IP addresses* parameter. By default, data is not collected.
Monitoring	
Select computers from the repository	Click **Browse [...]** to search the AppManager repository for the computers you want to monitor. You can select computers by view (for example, Master or NT), by server group, or individually. You can use this parameter as the sole selection method, or you can use it in conjunction with the *Computers to monitor* and *Filename for computer list* parameters. **Note** Once you specify a list of computers with this parameter, the script always monitors a list of computers generated by this parameter. You can modify the list, but you cannot delete it. If you want to subsequently specify monitored computers without using this parameter, you need to run a new monitoring job with this script and leave this parameter blank.
Computers to monitor (separate with comma, no space)	Specify a list of computers to monitor. Separate multiple names with commas and no spaces. For example, to check whether the Sales1 server can communicate with the computers `JOE`, `SAM`, and `PAT`, run this script on the `Sales1` computer and enter `JOE,SAM,PAT` in this field. You can use this parameter as the sole selection method, or you can use it in conjunction with the *Select computers from the repository* and *Filename for computer list* parameters.

Filename for computer list	Specify the path to the file that contains a list of computers you want to monitor, or click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<path to file>` rather than `\\<server>\D$\<path to file>`.
	The file should contain the hostname or IP address for each computer in one or more lines. Each line can have multiple computer names, separated by commas and no spaces.
	For example:
	`NYC01,NYC02`
	`SALES01,10.15.221.5, SFO01`
	`LABMACH,QATEST`
	You can use this parameter as the sole selection method, or you can use it in conjunction with the *Select computers from the repository and Computers to monitor* parameters.

Parameter	How to Set It
Router IP addresses (separate with comma, no space)	Specify the IP addresses of the routers through which the computer running the script should communicate with the target computers. **Note** If one of the listed routers is down, none of the target computers will be monitored.
Number of seconds to wait for ping response	Set the maximum number of seconds to wait for a response from a target computer. The default is 3 seconds.

MachineDownLR

Use this Knowledge Script to detect whether the computer on which you run the script can communicate with one or more remote Windows computers. This script requires that you first use the ConfigMachineDown Knowledge Script to store a list of remote computers in the local repository on the managed client computer where this script runs.

This script does **not** require the AppManager agent to be installed on the remote computers you want to monitor.

To run this script on a Windows Vista computer, the Remote Registry service on the agent computer must be running to connect to the Windows registry on the remote computers you want to monitor. If the Remote Registry Service is down when this script runs, an event is raised to indicate the remote computer was unresponsive and the connection to the Windows registry failed.

Once you have run ConfigMachineDown on each computer in a group, you can use MachineDownLR in a monitoring policy for the group. On each computer, the script knows what to monitor because ConfigMachineDown previously stored that information in the local repository. The use of MachineDownLR is the same as for MachineDown.

Note that this script displays event information in the Operator Console even if the remote computer is in maintenance mode.

Example of How this Script Is Used

If you want each computer in your environment to be able to check whether other selected computers are down, run ConfigMachineDown on each computer and specify the particular machine list you want that computer to monitor.

You can then put the MachineDownLR jobs in a monitoring policy that covers all those computers. As the job runs on each computer, it picks up the machine list from the local repository where ConfigMachineDown set it.

In this way, each instance of MachineDownLR can check a different list of computers from each computer where it runs.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data for computer availability?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following: • **100** -- target computer is up, • **0** -- the target computer is down, or • **50** -- communication failed (for example, because a computer's IP address is not found). The default is n.
Event severity when computer is down	Set the severity level, from 1 to 40, to indicate the importance of an event in which the target computer is down. The default is 5 (red event indicator).
Ping router?	Set to **y** to routinely ping the default gateway router. If enabled and the ping fails, the script stops and raises an event. The default is n. When this script runs, it first pings the default gateway router if the Ping Router parameter is enabled. If the ping fails, an event is raised. If the ping is successful or if no ping is requested, this script checks the registry of the destination computer. If that check fails, an event is raised. It also traces the route to the destination if the Trace the route parameter is enabled. If the registry check succeeds, communication with that computer is verified.
Number of seconds to wait for ping response	Specify the maximum number of seconds to wait for the ping to return a positive result. If the *Ping router* parameter is set to n, this threshold parameter is ignored. The default is 3 seconds.
Trace the route to a destination computer	Set to **y** to trace the route to a computer that is down. A traceroute can help you determine where the problem lies. The default is n.
Raise single event for all computers that are down?	Set to **y** to raise a single event regardless of the number of computers that are down. Set to **n** to raise a separate event for each computer that is down. The default is n.

MissingEvent

Use this Knowledge Script to determine whether a Windows event log does not contain an expected entry. This script raises an event if the Application, Security, or System event log does not contain an entry that matches your filtering criteria. You can use regular expressions or text/numeric strings to specify filtering criteria.

For more information, see "Creating Filters with Regular Expressions" on page 2059.

For example, the SQL backup process normally adds an entry to the event log to indicate databases were successfully backed up. This script can search for log entries that match your filtering criteria and raise an event if the event log does *not* contain an entry for a successful SQL backup.

To determine whether a Windows event log *does* contain an entry matching your filtering criteria, use the EventLog Knowledge Script.

Note
If you use text/numeric strings in the *Event [...] filter* parameters, this script searches event logs and matches the filter string to any part of the event entry. The results are not exact matches. For example, if your filter string is "foo," results will include "foobar," "foo," and "food."

Results for regular expression filters are exact matches.

Resource Objects

Windows computer or application server, such as Exchange Server or SQL Server

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MissingEvent job fails. The default is 25.
Event Log Monitoring	
Event logs to monitor	Indicate the name of the event log you want to monitor, separating multiple names with a comma. For example: `System,Application,Security` The default is `Application`. **Note** If the event log you specify does not exist on the target computer, the Application log is automatically monitored.

Parameter	How to Set It
Number of hours to scan logs	Set this parameter to control how the script scans the logs in the first interval, after which scanning begins where the previous scan ended. Enter one of the following values: • **-1** -- to scan all the existing entries • ***N*** -- to scan entries only for the past *n* hours (8 for the past 8 hours, 50 for the past 50 hours, for example) • **0** -- to not scan previous entries; only search from this moment on The default is 0.
Event Log Filters	
Use regular expressions for filter criteria?	Select **Yes** to use a regular expression to specify the criteria to look for in each event log you want to monitor. The default is unselected. You can use regular expressions in the *Event [...] filter* parameters, or you can create an external `.txt` file that contains the regular expressions you want to use as filtering criteria.
Enforce case sensitivity in regular expressions?	Select **Yes** to enforce case-sensitivity in all regular expressions used in the filter parameters or in the external `.txt` file. The default is unselected.
Event type for regular expression filtering	Use a regular expression to identify the type of event entries to search for in the logs: Error, Warning, Information, Audit_Success, Audit_Failure, Unclassified.
Path to file containing regular expression filters	Provide the full path to a file containing the regular expression filtering criteria you want to find in each monitored event log. For example: `C:\TEMP\MyFilters.txt`. Format the contents of the `.txt` file as described in "Using an External Filter File" on page 2094. **Note** If you specify a filter file, AppManager ignores the *Event [...] filter* parameters, even if the filter file is inaccessible for any reason, but continues to scan the log file specified in the *Event logs to monitor* parameter.
Event Types	
Error	Select **Yes** to search for log entries with an event type of Error. The default is Yes.
Warning	Select **Yes** to search for log entries with an event type of Warning. The default is Yes.
Informational	Select **Yes** to search for log entries with an event type of Informational. The default is Yes.
Success Audit	Select **Yes** to search for log entries with an event type of Success Audit. A Success Audit event is an audited security access attempt that succeeds. The default is Yes.
Failure Audit	Select **Yes** to search for log entries with an event type of Failure Audit. A Failure Audit event is an audited security access attempt that fails.The default is Yes.
Unclassified	Some events written to Windows event logs do not have event levels or severities set to event types recognized by Windows Server 2008 and later. This Knowledge Script identifies these entries as unclassified. These entries will not be found by the error, warning, informational, success audit, or failure audit filter criteria. Set to **Yes** to monitor log entries that are unclassified. The default is Yes.

Parameter	How to Set It
Event source filter	To search for log entries generated by a particular source (such as SQLExecutive, SNMP, or the Service Control Manager), enter a search string or a regular expression. This script will look for matching entries in the event log's Source field. Separate multiple strings with commas.
Event category filter	To search for log entries in a particular category (such as Server or Logon), enter a search string or regular expression. This script will look for matching entries in the event log's Category field. Separate multiple strings with commas.
Event ID filter	To search for log entries with particular event IDs, enter a search string, regular expression, or ID range (for example 100-2000). This script will look for matching entries in the event log's Event field. Separate multiple IDs and ranges with commas. For example: `1,2,10-15,202`.
Event user filter	To search for log entries associated with a particular user, enter a regular expression or search string, for example, `<domainname>\<username>`. This script will look for matching entries in the Event log's User field. Separate multiple strings with commas.
Event computer filter	To search for log entries generated by a particular computer, enter a search string or regular expression. This script will look for matching entries in the event log's Computer field. Separate multiple strings with commas.
Event description filter	To search for log entries with a particular detail description or containing keywords in the description, enter a search string or regular expression. This script will look for matching entries in the event log's Description field. Separate multiple strings with commas.
Event Notification	
Raise event if entries are missing from event logs?	Select **Yes** to raise an event if the selected event logs *do not* contain entries matching your filtering criteria. The default is Yes.
Event severity when entries are missing from event logs	Set the severity level, from 1 to 40, to indicate the importance of an event in which the selected logs do not contain entries matching your filtering criteria. The default is 5.
Data Collection	
Collect data for missing log entries?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of log entries found that match the filtering criteria. If no entries match the criteria, data collection returns 0 (zero). The default is unselected.
Separate data by log file type	Select **Yes** to separate event entries from different log files into different data streams. If disabled, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. For example, if you are monitoring both the System and Application logs, you can enable this parameter so that events in the System log are tracked separately from events in the Application log. The default is Yes.

Using an External Filter File

With the MissingEvent script, you can specify regular expressions for each *Event [...] filter* parameter or maintain your search criteria independent of the Knowledge Script parameters in a separate filter file.

In many cases, specifying an external filter file provides greater flexibility and makes modifying your search criteria more straightforward because you can add almost any number of expressions and you do not need to modify the Knowledge Script properties to pick up your changes.

Note
If you specify a filter file, AppManager ignores the *Event [...] filter* parameters, even if the filter file is inaccessible for any reason.

If you want to use a filter file:

- Identify the strings that you want to find a match for, that is, the entries you want to include in your results.
- Create a text file with one regular expression string per line to locate matching strings. Each line in the file consists of a parameter keyword followed by a colon (:), a tab or blank space, and the regular expression. Or the filter file can be written using XML.
- Make sure the file exists on the target computer.
- Type the absolute path to the file on the local computer in the *Path to file containing regular expression filters* parameter and start the job.

Two formats are valid for the filter file: a simple table format to define the strings to include and an XML format that allows you to define more complex include and exclude filtering. For both formats, the parameter name keywords are required, but the field values can be left blank if no filtering is needed.

Select a format appropriate for the complexity of your filtering needs.

Table Format

The table format provides a simple way to create the filter file. Each filtering section in the file begins with `EventStart` and ends with `EventEnd`. If an entry in the event log matches all the criteria you have specified within a filtering section, it is considered a match; no AppManager event is raised. If you have more than one filtering section, a log entry can match either section. Remember, for the MissingEvent Knowledge Scripts, events are raised only when no log entry matches your criteria.

For example, the following table format file provides two filter sections:

```
EventStart
CaseSensitive:n
Log:System
Type:Error|Warning|Information
Source:^SQL*
Category:*
EventID:1[0-9][0-9][0-9]
User:Sam|Joe|Chris
Computer:SFO*
Description:($Error.*)|(.*error.*occurred.$)
EventEnd
EventStart
CaseSensitive:n
Log:Application
Type:Error|Warning|Information
Source:^SQL*
Category:*
EventID:1[0-9][0-9][0-9]
User:Sam|Joe|Chris
Computer:SFO*
Description:($Error.*)|(.*error.*occurred.$)
```

```
EventEnd
```

Note
If you are only specifying one filter section, do not include the `EventStart` and `EventEnd` lines in the file.

XML Format

The XML format is more sophisticated and more flexible than the table format. The XML format allows you to set both include and exclude filters using the `<Include>` and `<Exclude>` tags and to combine these filter sets to define the search criteria. Each filtering section in the file begins with the `<Events>` tag. A log entry must match all the criteria you specified within a filtering section for it to be considered a match.

For example:

```
<?xml version = "1.0" standalone = "yes"?>
<EventLogConfig Name = "Event Filter" Type = "EVENT_FILTER_CUSTOM" ID = "76">
<Include>
   <Events>
      <Log>Application</Log>
      <Type>INFORMATION|WARNING|ERROR</Type>
      <Source><Net*]></Source>
      <Category>*</Category>
      <EVENTID>2*</EVENTID>
      <User>*</User>
      <Computer>*</Computer>
      <Description><![CDATA[Event.]]></Description>
      <CaseSensitive>y</CaseSensitive>
   </Events>
   <Events>
      <Log>System</Log>
      <Type>Warning</Type>
      <Source>RSVP</Source>
      <Category>*</Category>
      <EVENTID>*</EVENTID>
      <User>*</User>
      <Computer>SHASTA</Computer>
      <Description>RSVP*</Description>
      <CaseSensitive>y</CaseSensitive>
   </Events>
</Include>
</EventLogConfig>
```

Note
If a field contains a regular expression that conflicts with XML syntax or includes special characters, you can use `![CDATA[regular_expression]]` to enclose the expression and prevent parsing problems.

PingMachine

Use this Knowledge Script to check the availability of computers or other machines that reply to ICMP Echo requests. With this script, you can use your managed client Windows computer to check the up/down status of UNIX computers, other Windows computers, and other equipment, such as TCP/IP-based printers. The ICMP Echo request is commonly used by the ping command on UNIX and Windows computers.

This script automatically raises an event if a computer does not respond to the ping command from the computer where this script is running. Note that this script returns event information even if the remote computer is in maintenance mode. In addition, you can choose to raise an event if the ping attempt fails for any other reason.

When configuring an action for this script, configure the Location to initiate the action on the MS (management server) or on a Proxy (to run on a particular managed client computer).

If you configure an action to run on the managed client (MC), when a remotely monitored computer is placed into machine maintenance mode or scheduled maintenance mode, any event conditions detected on the remote computer are ignored but the action is not disabled; in this case, an action is run but there will be no event information on the Events tab of the Operator Console.

Note
This script does not require the AppManager agent to be installed on the remote computers you want to monitor.

Resource Objects

Any Windows server that recognizes the ping command

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
List of computers to check	Specify a list of the computer names or hostnames, separated by commas, to which you want to test communication. For example, to check connectivity to the NetIQ Corporation Web site, type: `www.netiq.com`. You can specify computers that are not currently in the TreeView pane of the Operator Console.

Full path to file with list of computers	Provide the full path to the file containing a list of the computers to check. The file should contain the hostname or IP address for each computer in one or more lines. Each line can have multiple computer names, separated by commas. For example:
	`NYC01,NYC02`
	`SALES01,10.15.221.5, SFO01`
	`LABMACH, QATEST`

Number of seconds to wait for ping response	Specify the maximum number of seconds to wait for a response before timing out. The default is 3 seconds.

Parameter	How to Set It
Number of echo requests to send	Specify the maximum number of times to send the ping request before raising an event. The default is 2 times.
Threshold - Maximum number of consecutive timeouts	Specify the maximum number of consecutive timeouts to allow before raising an event. The default is 1 timeout.
Raise event for any errors during ping?	Select **Yes** to raise an event if an error other than timing out occurs during the ping attempt. The default is Yes.
Event severity for ping errors	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an error other than timing out occurs during the ping attempt. The default is 5 (red event indicator).
Data Collection	
Collect data for computer availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the target computer responded to the ping • **0** -- the target computer did not respond • **50** -- either the ping failed or the ping returned no output to the results file The default is y.
Collect data for response time?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average response time for the computers to which a ping request has been sent. If a computer is unavailable or a ping error occurs, response time data collection returns 0. Ping response times of less than 1 ms are returned as 1 ms.

Report_MachineAvailability

Use this Knowledge Script to generate a report about the availability of computers. This report uses data collected by the MachineDown Knowledge Script, which tests the connection from a single computer to one or more other computers.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select computers	Select the computers whose data you want to include in your report.
Select time range	Set a specific or sliding time range for data included in your report. The default is a sliding time of 1 day.
Select peak weekdays	Select the days of the week to include in your report. The default is seven days: Sunday through Saturday
Data settings	
Hours or percentage on chart	Select whether to illustrate availability by hours or by percentage. The default is Percentage.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted. This is the default option. • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is yes.
Report settings	
Include parameter help card?	Select **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.

Parameter	How to Set It
Include table/chart/both?	Select an option to include data stream values in the report: • **Table: Select this option to include a table of data stream values in the report.** • **Chart:** Select this option to include a chart of data stream values in the report. • **Both:** Select this option to include both table and chart of data stream values in the report.
Select chart style	Define the graphic properties of the charts in your report. The default chart style is Pie.
Select output folder	Set parameters for the output folder. The default folder name is General_MachineAvailability.
Add job ID to output folder name?	Select **yes** to add the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set report properties. The default report name is General Machine Availability.
Add time stamp to title?	Select **yes** to add a time stamp to the title of the report, making each title unique. The time stamp shows the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Select **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_PingMachine

Use this Knowledge Script to generate a report about the availability of computers or other machines that reply to ICMP Echo requests. This report uses data collected by the PingMachine Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select time range	Set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending in 24 hours.
Select peak weekday(s)	Select the days of the week to include in your report. The default is seven days: Sunday through Saturday.
Data settings	
Hours or percentage on chart	Select whether to illustrate availability by hours or by percentage. The default is Percentage.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default) The default is No Sort.
Percentage/count for top/bottom	Specify a value for the percentage or count defined in the *Select sorting/display option* parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is yes.
Report settings	
Include parameter help card?	Select **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.

Parameter	How to Set It
Include table/chart/both?	Select an option to include data stream values in the report: • **Table: Select this option to include a table of data stream values in the report.** • **Chart:** Select this option to include a chart of data stream values in the report. • **Both:** Select this option to include both table and chart of data stream values in the report.
Select chart style	Define the graphic properties of the charts in your report. The default chart style is Pie.
Select output folder	Set parameters for the output folder. The default folder prefix is General_PingMachine.
Add job ID to output folder name?	Select **yes** to add the job ID to the name of the output folder. By default, the job ID is not included. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Set report properties. The default title for your report is General Ping Machine Availability.
Add time stamp to title?	Select **yes** to add a time stamp to the title of the report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Select **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ServiceChange

Use this Knowledge Script to generate a report about changes to the status and start-type of discovered services. This report uses data collected by the ServiceChange Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select time range	Set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending in 24 hours.
Select peak weekday(s)	Select the days of the week to include in your report. The default is seven days: Sunday through Saturday.
Data settings	
Hours or percentage on chart	Select whether to illustrate availability by hours or by percentage. The default is Percentage.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default) The default is No Sort.
Percentage/count for top/bottom	Specify a value for the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Report settings	
Include parameter help card?	Select **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.

Parameter	How to Set It
Include table/chart/both?	Select an option to include data stream values in the report: • **Table: Select this option to include a table of data stream values in the report.** • **Chart:** Select this option to include a chart of data stream values in the report. • **Both:** Select this option to include both table and chart of data stream values in the report. The default is Table.
Select chart style	Define the graphic properties of the charts in your report. The default chart style is Pie.
Select output folder	Set parameters for the output folder. The default report prefix is General_ServiceChange.
Add job ID to output folder name?	Select **yes** to add the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set report properties. The default report title is General Service Change.
Add time stamp to title?	Select **yes** to add a time stamp to the title of the report, making each title unique. The time stamp shows the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Select **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ServiceDown

Use this Knowledge Script to generate a report about the up/down status of discovered services. This report uses data collected by the ServiceDown Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select time range	Set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending in 24 hours.
Select peak weekday(s)	Select the days of the week to include in your report. The default is seven days: Sunday through Saturday.
Data settings	
Hours or percentage on chart	Select whether to illustrate availability by **Hours** or by **Percentage**. The default is Percentage.
Select sorting/display option	Select whether data is sorted, and the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, the data table shows only the top or bottom N or % (for example, only the top 10%). If set to no, the table shows all data. The default is yes.
Report settings	
Include parameter help card?	Select **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.

Parameter	How to Set It
Include table/chart/both?	Select an option to include data stream values in the report: • **Table: Select this option to include a table of data stream values in the report.** • **Chart:** Select this option to include a chart of data stream values in the report. • **Both:** Select this option to include both table and chart of data stream values in the report.
Select chart style	Define the graphic properties of the charts in your report. The default chart style is Pie.
Select output folder	Set parameters for the output folder. The default report prefix is General_ServiceDown.
Add job ID to output folder name?	Select **yes** to add the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set report properties. The default report title is General Service Down.
Add time stamp to title?	Select **yes** to add a time stamp to the title of the report, making each title unique. The time stamp shows the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Select **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ServiceHung

Use this Knowledge Script to generate a report about discovered services in the Start-Pending, Stop-Pending, Continue-Pending, or Pause-Pending state. If a service is detected in one of these states for a specified number of intervals, it is considered hung. The number of intervals is specified in the Knowledge Script that collects data for this report.

This report uses data collected by the ServiceHung Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select time range	Set a specific or sliding time range for data included in your report. The default is a sliding time of 1 day.
Select peak weekday(s)	Select the days of the week to include in your report. The default is seven days: Sunday through Saturday.
Data settings	
Hours or percentage on chart	Select whether to illustrate availability by **Hours or** by **Percentage**. The default is Percentage.
Select sorting/display option	Select whether data is sorted, and the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, the data table shows only the top or bottom N or % (for example, only the top 10%). If set to no, the table shows all data. The default is yes.
Report settings	
Include parameter help card?	Select **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.

Parameter	How to Set It
Include table/chart/both?	Select an option to include data stream values in the report: • **Table: Select this option to include a table of data stream values in the report.** • **Chart:** Select this option to include a chart of data stream values in the report. • **Both:** Select this option to include both table and chart of data stream values in the report.
Select chart style	Define the graphic properties of the charts in your report. The default chart style is Pie.
Select output folder	Set parameters for the output folder. The default report prefix is General_ServiceHung.
Add job ID to output folder name?	Select **yes** to add the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set report properties. The default report title is General Service Hung.
Add time stamp to title?	Select **yes** to add a time stamp to the title of the report, making each title unique. The time stamp shows the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Select **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

ServiceChange

Use this Knowledge Script to detect any changes to the status and start type of a discovered service. You can run this script for almost any service, including SQL Services, Exchange Services, and IIS Services. This script raises an event if the status (running, stopped, pending, and so on) or startup type (manual, automatic, disabled) of any service has been changed.

Resource Objects

Windows computer or Windows application service

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data for service changes?	Set to **y** to collect data for charts and reports. If enabled, data collection returns one of the following: • **100** -- the service is unchanged • **0** -- the service is not running or has been changed. The default is n.
Event severity when service start type changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service's start type has changed. The default is 10 (red event indicator).
Event severity when service status changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service's status has changed. The default is 5 (red event indicator).
Event severity when information retrieval fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the script failed to retrieve service information. The default is 18 (yellow event indicator).

ServiceDown

Use this Knowledge Script to detect whether a discovered service is running. You can run this script for most services, including SQL Server services, Exchange Server services, and IIS services. Use the NT_ServiceDown Knowledge Script to check other services, such as `WinLogon` or `NetIQms`, which are not included in the Operator Console TreeView.

This script raises an event if any monitored service is not running and can automatically restart the down service.

Resource Objects

Windows computer or Windows application service

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if service is stopped?	Select **Yes** to raise an event if the status of a monitored service is "stopped." The default is Yes.
Event severity when service is stopped	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a monitored service is "stopped." The default is 18 (yellow event indicator).
Event severity when service cannot be started	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this script is unable to start a stopped service. The default is 5 (red event indicator).
Raise event if service is started?	Select **Yes** to raise an event if this script successfully starts a stopped service. The default is unselected.
Event severity when service is started	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this script successfully starts a stopped service. The default is 25 (blue event indicator).
Raise event if service is missing?	Select **Yes** to raise an event if a service that was found during a previous discover cannot be found. The default is unselected.
Event severity when service is missing	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a discovered service is missing. The default is 8 (red event indicator).
Raise event if service is disabled?	Select **Yes** to raise an event if a service is stopped and is disabled. The default is unselected.
Event severity if service is disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is stopped and is disabled. The default is 12 (yellow event indicator).

Parameter	How to Set It
Raise event if service is shut down normally?	Select **Yes** to raise an event if a service was stopped as a result of a stop request, such as a stop request issued by a user or as a result of another service being stopped. The default is Yes. This parameter takes effect only when the *Only restart service if shut down normally?* parameter is disabled.
Event severity when service shut down normally	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service was stopped as a result of a stop request. The default is 30 (blue event indicator).
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ServiceDown job fails. The default is 5 (red event indicator). An event is raised for circumstances under which the script fails to run properly.
Data Collection	
Collect data for service status?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns one data stream for each service you are monitoring, and, for each monitored service, one data stream covering all dependent services. For monitored services, the data detail message includes the service name, the start type, and the status. If a monitored service is up, a value of 100 is returned. If the service is down, a value of 0 is returned. If the service is down and the Knowledge Script successfully restarts the service, a value of 50 is returned. For services depending on the monitored service, the data detail message includes service names, and the start type and status of each service. If all dependent services are up, a value of 100 is returned; if any dependent service is down, a value of 0 is returned. The default is unselected.
Monitoring	
Start stopped services?	Select **Yes** to start a service that is not running. The default is Yes.
Number of seconds to wait for service start	Specify the number of seconds this script should attempt to start a service before timing out. The default is 30 seconds. **Note** If the service fails to start within the timeout period, an event is raised if the *Raise event if service is down?* parameter is set to Yes. The severity of the event is determined by the *Event severity when service cannot be started* parameter.
Start dependent services? (6.0+)	Select **Yes** to start any service that depends on other services started by this script. For example, if this script starts the `MSSQLSERVER` service, it will also start the dependent `SQLSERVERAGENT` service. The default is Yes.
Restart service if shut down normally? (5.0+)	Select **Yes** to restart a service that was stopped as a result of a stop request, such as a stop request issued by a user or as a result of another service being stopped. The default is Yes.

ServiceHung

Use this Knowledge Script to detect whether a discovered service is hung. You can run this script for most services, including SQL Services, Exchange Services, and IIS Services. A service is considered hung if it is in a Start-Pending, Stop-Pending, Continue-Pending or Pause-Pending state for a specified number of consecutive intervals. This script raises an event if a hung service is detected, and can stop or restart the hung service.

Resource Objects

Any discovered Windows computer or Windows application service

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Number of consecutive iterations before service is hung	Specify the number of consecutive job iterations a service can be in a Start-Pending, Stop-Pending, Continue-Pending or Pause-Pending state before it is considered hung. The default is 2 consecutive iterations.
Collect data for service status?	Set to **y** to collect data for charts and reports. If enabled, data collection returns one of the following: • **100** -- service is up • **0** -- service is hung The default is n.
Stop the hung service?	Set to **y** to automatically stop hung services. The default is y.
Start hung service after it is stopped?	Set to **y** to automatically start the service after stopping it. The default is y.
Event severity when start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this script fails to start a hung service that had been stopped. The default is 5 (red event indicator).
Event severity when start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this script successfully starts a hung service that had been stopped. The default is 25 (blue event indicator).
Event severity when “start hung service” is disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the a hung service is detected and the *Start hung service after it is stopped?* parameter is set to n. The default is 18 (yellow event indicator).
Event severity when status retrieval fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this script cannot determine the status of a service. The default is 10 (red event indicator).
Event severity when service stop fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this script fails to stop a hung service. The default is 8 (red event indicator).

ShortEventLog

Use this Knowledge Script to track Windows event log entries that match filtering criteria you specify. This script works on an incremental basis (it does not fully rescan the event log each time it runs), and all event log entries that match the filtering criteria are returned in the event or data point detail message.

This script works in the same fashion as the EventLog Knowledge Script, but removes the header information and returns only the description of the event.

Note
Only the most recent batch of events can be viewed in the data point detail message. For example, you might set this script to scan all previous entries in the event log and list ten matching entries in each event detail message. When the job runs, 30 entries are found that match your filtering criteria. In this case, the script creates three child events for the interval. Each child event contains ten entries: the oldest matching entries in one child event batch, the second oldest in Batch 2, and the most recent in Batch 3. If this job is collecting data, and you view the data detail message for the interval, only the entries from the third child event (Batch 3) are displayed.

Resource Objects

Windows computer or application server such as Exchange Server or SQL Server

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if log entries match criteria?	Set to **y** to raise an event when log entries match your filtering criteria. The default is y.
Collect data for log entries that match criteria?	Set to **y** to collect data for charts and reports. When enabled, data collection returns detail about log entries that match your filtering criteria. The default is n.
Separate data by log file type?	Set to **y** to separate event entries from different log files into different data streams. If set to n, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. For example, if you are monitoring both the System and Application logs, you can enable this parameter so that events in the System log are tracked separately from events in the Application log. The default is n.
Log files to filter (Application, Security, System)	Specify the event log you want to monitor. You can specify multiple event logs, separated by commas. For example: `System,Application,Security` The default is `Application`.

Parameter	How to Set It
Log scanning for first interval	Set this parameter to control how the script scans the logs at the first interval, after which scanning begins where the previous scan ended. Enter one of the following values: • **-1** -- to scan all the existing entries • ***N*** -- to scan entries only for the past *n* hours (8 for the past 8 hours, 50 for the past 50 hours, for example) • **0** -- to not scan previous entries; only search from this moment on. The default is 0.
Monitor error events?	Set to **y** to monitor error event entries. The default is y.
Monitor warning events?	Set to **y** to monitor warning event entries. The default is y.
Monitor information events?	Set to **y** to monitor information event entries. The default is y.
Monitor success audits?	Set to **y** to monitor success audit event entries. Success audits are successful security access attempts that are audited. The default is y.
Monitor failure audits?	Set to **y** to monitor failure audit events entries. Failure audits are failed security access attempts that are audited. The default is y.
Event source filter	To filter for events generated by a particular source (such as SQLExecutive, SNMP, or the Service Control Manager), enter a search string. This script will look for matching entries in the Event Log's **Source** field. Separate multiple strings with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary
Event category filter	To filter for events in a particular category (such as Server or Logon), enter a search string. This script will look for matching entries in the Event Log's **Category** field. Separate multiple strings with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.
Event ID filter	To filter for particular event IDs, enter a search string or ID range, for example 100-2000. This script will look for matching entries in the Event Log's **Event** field. Separate multiple IDs and ranges with commas. For example: `1,2,10-15,202`. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.
Event user filter	To filter for events associated with a particular user, enter a search string, for example, `<domain name>\<user name>`) This script will look for matching entries in the Event Log's **User** field. Separate multiple strings with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary
Computer filter	To filter for events generated by a particular computer, enter a search string. This script will look for matching entries in the Event Log's **Computer** field. Separate multiple strings with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.

Parameter	How to Set It
Event description filter	To filter for events with a particular detail description or containing keywords in the description, enter a search string. This script will look for matching entries in the Event Log's **Description** field. Separate multiple strings with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you specify only include criteria, the colon is not necessary.
Maximum number of entries per event report	Specify the maximum number of entries to be recorded in each event's detail message. If this script finds more entries from the log than can be put into one event message, it will return multiple events to report all the outstanding entries in the log. The default is 30 entries. If this script encounters one or more very large events in the Windows Event log, this Knowledge Script may error out and generate an event message "`Out of string space`." If this occurs, you can usually work around the problem by adjusting this parameter to a smaller value.
Event severity when event log entries match criteria	Set the event severity level, from 1 to 40, to indicate the importance of an event in which log entries matched your search criteria. The default is 8 (red event indicator). **Tip** You can adjust the severity based on which log or type of event you are checking for.

Examples of How this Script Is Used

You can customize this script in many ways based on your requirements. For example, for general system events, you can set the following options when detecting security failures:

Properties and Parameters	How You Might Set Them
Schedule interval	10 minutes
Raise event if log entries match criteria?	y
Log files to filter	Security
Monitor failure audits?	y
Event severity when event log entries match criteria	2
Action	MapiMail

With this scenario, on the **Schedule** tab in the Knowledge Script Properties dialog box, set the interval to *Once very 10 minutes* because you want a short window for checking for this type of problem.

On the Values tab, enable the *Raise event if log entries match criteria?* parameter. Set *Log files to filter* to **Security** and set *Monitor failure audits?* to **y**. Set the *Event severity level* parameter to **2**, indicating this is a very serious event that you want to be highly visible. Leave the other filtering options blank.

On the **Action** tab, indicate that you want an e-mail sent if an event is raised. With these settings, AppManager for Microsoft Windows will regularly check for security failures and will notify you, or whoever you designate, through e-mail if any security failure events are detected.

Another example of how to use this script to detect all problems with your SQL Server involves setting up the Knowledge Script job as follows:

Properties and Parameters	How You Might Set Them
Schedule interval	30 minutes
Raise event if log entries match criteria?	y
Log files to filter	Application
Monitor error events?	Error
Event source filter	MSSQLServer
Event severity when event log entries match criteria	8
Action	MapiMail

Another way you can use this Knowledge Script is to collect data and graph a trend chart from your System event log:

Properties and Parameters	How You Might Set Them
Schedule interval	1 hour
Collect data for log entries that match criteria?	y
Log files to filter	System
All other filters	not set
Action	Null

If you select the data collection option, this script returns the number of matched entries as the primary data point to be graphed. The first batch of filtered results can be viewed in the detail data message when you double-click a data point. Additional matching entries may be included in the graph. The peaks and valleys in the graph indicate a large number of events (something unusual) or low event activity (quiet and all "OK").

SNMPGet

Use this Knowledge Script to monitor SNMP activity for the device or computer you specify. This script performs an SNMP v1 `Get` or `GetNext` against the selected SNMP agent, allowing you to check SNMP MIB (management information base) variable values. The value returned can be compared to the thresholds you set or a text string. This script requires the Microsoft SNMP Service to be running.

Note
When setting the parameters for this script, choose whether the jobs should perform a threshold comparison, equality check, or string matching. These operations are mutually exclusive operations.

Resource Objects

Any Windows server or CIM server with an SNMP agent installed and running

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if MIB variable matches string or numeric value, or exceeds or falls below threshold?	Set to **y** to raise an event if a MIB value falls below or exceeds the threshold, or if a value matches the parameters you set for *Equality check?* or *String match*. The default is y.
Collect data for MIB variable?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the value of the MIB variable for graphing. If the MIB variable you specify is of an octet string type, the value is displayed in the graph data detail message. The default is y.
MIB object identifier	Specify a MIB object identifier in OID notation (for example, `.1.2.3.456.78`) or ODE notation (for example, `system.sysUpTime.0`). The default is `system.sysName.0`. OID notation must include the dot (.) at the beginning of the identifier. ODE notation must be case-sensitive. You can use the ODE if the `mib.bin` file has been compiled on the agent computer in the `%windir%/system32` directory. For information about compiling the `mib.bin`, see the Windows Resource Kit.
SNMP community string	Provide the SNMP community string for the device or computer on which you want to monitor SNMP activity. Leave this parameter blank to use the SNMP community name entered in the AppManager for Microsoft Windows Security Manager. The default is `public`.
SNMP agent	Specify the hostname or IP address of the device or computer on which you want to monitor SNMP activity. If you do not specify an SNMP agent, the local client computer is assumed.
Threshold - Maximum MIB variable value	Specify the maximum value the MIB variable can attain before an event is raised. The default is 600000.
Threshold - Minimum MIB variable value	Specify the minimum value the MIB variable must maintain to prevent an event from being raised. The default is 300000.

Parameter	How to Set It
Check for equality to numeric MIB variable	• Set to **e** to compare the MIB variable's value to a specific value (set in the *Numeric MIB variable value* parameter) and raise an event when the values are equal. • Set to **n** to compare the MIB variable's value to a specific value (set in the *Numeric MIB variable value* parameter) and raise an event when the values are not equal. • Set to **s** to skip testing for equality. This parameter is applicable for numeric MIB variables such as `INTEGER`, `GAUGE`, or `COUNTER`. The default is s.
Numeric MIB variable value	Specify the value that you want to compare with the returned MIB variable value. • If *Check for equality to numeric MIB value?* is set to **e**, an event is raised when the MIB variable equals the value you specify in this parameter. • If *Check for equality to numeric MIB value?* is set to **n**, an event is raised when the values are not equal. The default is 0.
Text string or IP address MIB variable value	Specify the text string or IP address that you want to compare with the returned MIB variable value. This parameter is applicable only when the MIB type is `OCTETSTRING` or `IPADDRESS`. The MIB variable value is compared to this string, and an event is raised if they are equal.
Enforce case-sensitive string match?	Set to **y** to enable this script to match case when checking for a match to the string entered for the *String match* parameter. The default is n.
Event severity when MIB variable matches string or numeric value, or exceeds or falls below threshold?	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a MIB variable value exceeds or falls below the threshold, or if a value matches the parameters you set for *Equality check?* or *String match*. The default is 5 (red event indicator).
Select operation: Get or GetNext	Specify whether to perform SNMP `Get` or `GetNext`. The default is `Get`.
Number of times to perform the operation	Specify the number of times this script should try to perform the `Get` operation before returning an error. The default is 3 times.
Number of seconds to wait for operation to complete	Specify the number of seconds this script should wait for the `Get` or `GetNext` operation to complete before timing out and returning an error. The default is 5 seconds.
Event message text	Provide the text to display in the event detail message. If you do not enter a message, a default message consisting of the MIB variable and value is used.

WMICounter

Use this Knowledge Script to monitor any Windows Management Instrumentation (WMI) object property. You can run this script on any WMI server and monitor any property available for an object. This script raises an event if the value of the property you select exceeds or falls below the threshold you set. You can also specify a consecutive number of times that the threshold must be exceeded before an event is raised.

Use this script to yield performance information for the WMI properties you are monitoring. Use the property data to start corrective actions when thresholds are exceeded, to generate complex and sophisticated graphs, and to provide historical information for reporting, trend analysis, and capacity planning.

Note
An event is raised only if the property value exceeds or falls below the thresholds you set. If a counter does not exist on the monitored computer, the job terminates with an error.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data for WMI object property values?	Set to **y** to collect data for charts and reports. When enabled, data collection returns the object property values that exceeded or fell below the threshold you set. The default is n.
Raise event when object property value exceeds threshold?	Set to **y** to raise an event if the object property value exceeds the maximum threshold you set. The default is y.
Threshold - Maximum value for object property	Specify the maximum value the object property can attain before an event is raised. The default is 100.
Raise event when object property value falls below threshold?	Set to **y** to raise an event if the object property value falls below the minimum threshold you set. The default is y.
Threshold - Minimum value for object property	Specify the minimum value the object property must maintain to prevent an event from being raised. The default is 10.
WMI object property to monitor	Specify the namespace, class, and property to monitor. For more information, see "Selecting a Property to Monitor Using the WMI Browser" on page 2120 and "Entering Property Names Without Browsing" on page 2120. For details about WMI classes and objects, see the WMI Object Browser available with the WMI platform SDK.

Parameter	How to Set It
Number of consecutive times to exceed or fall below threshold	Specify the number of consecutive times a monitored object property value should exceed or fall below the threshold before an event is raised. The default is 1 time.
Raise event if value cannot be retrieved?	Set to **y** to raise an event if this script cannot retrieve the object property value. The default is y.
Event severity when object property value exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the object property value exceeds the threshold you set. The default is 8 (red event indicator).
Event severity when object property value falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the object property value falls below the threshold you set. The default is 8 (red event indicator).
Event severity when property/instance not found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the the specified property or instance does not exist. The default is 8 (red event indicator).

Selecting a Property to Monitor Using the WMI Browser

To select the property you want to monitor, click **Browse [...]** in the *WMI object property to monitor* parameter to launch the Windows Management Instrumentation Browser dialog box. Specify the target computer, the namespace and class in which the property resides, the instance of the property, such as the name of a service or particular log file, and the name of the specific property you want to monitor. The term "schema" in this dialog box refers to properties.

To select a property to monitor using the WMI browser:

1. Click **Browse [...]** and select the target **Computer**.
2. From the **Classes In** list, specify the namespace that contains the class in which the object and property (schema) are located.
3. Click **Enumerate** to view the classes and objects in the namespace you specified.
4. Select the **Instance** of the class you want to monitor.
5. From the **Schema** list, select the name of the property you want to monitor.
6. Click **OK**.

Entering Property Names Without Browsing

To type property names rather than use the Windows Management Instrumentation Browser, enter the name in the *WMI object's property to monitor* parameter using the following format:

```
<namespace>:<class.instance="unique identifier">:<property>
```

where `instance` is the instance category (such as name or log file), and `"unique identifier"` is the name of the specific instance you want to monitor. Using the example from the previous section, to monitor the state of the `NetIQmc` service, type this information in the *WMI object's property to monitor* parameter as follows:

```
\\root\CIMV2:Win32_BaseService.name="NetIQmc":State
```

where

- `\\root\CIMV2` is the namespace
- `Win32_BaseService` is the class

- `name` is the instance
- `NetIQmc` is the unique identifier that specifies the specific service you want to monitor
- `State` is the property of the instance that you want to monitor

Chapter 38
HP SIM Knowledge Scripts

AppManager for Hewlett-Packard Systems Insight Manager (HP SIM) provides a set of Knowledge Scripts for monitoring servers running HP SIM. It also includes Knowledge Scripts to generate reports about the performance of your HP SIM implementation.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ArrayLogicalDriveCondition	Monitors the overall condition of logical drives in an array set.
ArrayLogicalDriveStatus	Monitors the status of logical drives in an array set.
ArrayPhysicalDiskStatus	Monitors the status of physical drives in an array set.
ASRHealth	Monitors Automatic Server Recovery (ASR) status and the number of ASR-initiated reboots.
ASRStatus	Monitors changes to the Automatic Server Recovery (ASR) status, and the status of the Pager, DialIn, and DialOut functions.
CorrectableMem	Monitors the condition of correctable memory and the number of new correctable memory errors.
CriticalErrorLog	Monitors the Critical Error Log for uncorrected critical error entries.
EventLog	Monitors NT event log entries created by SIM (entries with Insight Agents as the source).
FanIndividual	Checks the status of individual fans.
FanSummary	Monitors the status of System and CPU fans.
FCAExternalControllerFail	Monitors the operational status of Fibre Channel Array (FCA) external controllers.
FCAFail	Monitors the status of FCA controllers.
FCAHostControllerFail	Monitors the operational status of FCA host controllers.
FCAHostFail	Monitors the status of FCA host controllers.
FCAOverallCondition	Monitors the overall condition of the FCA system.
FLTPWRIndividualCondition	Monitors the status of fault tolerant power supplies.
FLTPWROverallCondition	Monitors the overall condition of the Fault Tolerant Power Supply sub-system.
HealthCheck	Monitors all SIM services and automatically restarts any service that is not running.
IDAFail	Monitors IDA controllers and IDA drives.

Knowledge Script	What It Does
IDEFail	Monitors IDE controllers and IDE drives.
IntegratedLog	Monitors the Integrated Management Log.
NICError	Monitors network interface transmission errors.
NICFail	Checks whether the network interface subsystem is down.
Report_ASRHealth-RebootCount	Generates a report about ASR status, and the number of ASR-initiated reboots.
Report_CIMResource_CPU_MemoryUsage	Generates a report about CPU and memory usage by SIM processes.
Report_CIMSCSI-Status	Generates a report about the number of hard resets, soft resets, and command timeouts for the SCSI controller.
Report_CorrectableMemoryErrors	Generates a report about the condition of correctable memory, and the number of new correctable memory errors.
Report_NewEventLogEntries	Generates a report about Windows event log entries with the SIM Insight Agent as the source.
Report_NICErrorRate	Generates a report about network interface input and output errors.
ResourceHigh	Monitors the CPU and memory used by the SIM process.
RIBBatteryRechargeLevel	Monitors the battery recharge level of the Remote Insight Board battery.
RIBBatteryStatus	Monitors the status of the Remote Insight Board battery.
RIBBatteryRechargeLevel	Monitors the status of the Remote Insight Board cable connections, including the keyboard, mouse and external power cable.
RIBCondition	Monitors the overall condition of the Remote Insight Board.
RIBInterfaceStatus	Monitors the interface status of the Remote Insight Board.
RIBVirtualPowerCable	Monitors the virtual power cable connection of the Remote Insight Board.
SCSIFail	Monitors discovered SCSI drives.
SCSITimeout	Monitors the number of hard resets, soft resets, and command timeouts for the SCSI controller during the monitoring interval.
TeamedNICCondition	Monitors the condition of Teamed NIC.The job raises an event when Teamed NIC is degraded or fails.
TempIndividual	Monitors the status of SIM temperature sensors.
ThermalStatus	Monitors the computer’s thermal environment and the status of the computer’s temperature sensors.
UPSBatteryLow	Monitors the UPS battery life.
UPSLineStatus	Checks the status of the UPS AC power line.

ArrayLogicalDriveCondition

Use this Knowledge Script to monitor the overall condition of logical drives in an array set. The job raises an event if a monitored logical drive is not operating properly.

Resource Object

Array Logical Drive object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is **n**.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Logical drive failed	Set the event severity level from 1 to 40, to indicate the importance of an event in which a logical drive in an array set failed. The default is 5.
Severity - Logical drive degraded	Set the event severity level from 1 to 40, to indicate the importance of an event in which a logical drive in an array set is in a degraded condition. The default is 12.
Severity - Unknown condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which a logical drive in an array set is in an unknown condition. The default is 15.
Severity - Unexpected Knowledge Script error	Set the event severity level from 1 to 40, to indicate the importance of an event in which the ArrayLogicalDriveCondition Knowledge Script fails unexpectedly. The default is 35.

ArrayLogicalDriveStatus

Use this Knowledge Script to monitor the status of logical drives in an array set. The job raises an event if the status of a monitored logical drive is anything but normal.

Resource Object

Array Logical Drive object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is **n**.
Event severity level for SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Event severity level for logical drive failed	Set the event severity level from 1 to 40, to indicate the importance of an event in which a logical drive in an array set failed. The default is 5.
Event severity level for logical drive not configured	Set the event severity level from 1 to 40, to indicate the importance of an event in which a logical drive in an array set is not configured. The default is 25.
Event severity level for logical drive recovering	Set the event severity level from 1 to 40, to indicate the importance of an event in which a logical drive in an array set is recovering. The default is 15.
Event severity level for logical drive ready for rebuild	Set the event severity level from 1 to 40, to indicate the importance of an event in which a logical drive in an array set is ready for rebuild. The default is 25.
Event severity level for logical drive rebuilding	Set the event severity level from 1 to 40, to indicate the importance of an event in which a logical drive in an array set is being rebuilt. The default is 15.
Event severity level for wrong physical disk replaced	Set the event severity level from 1 to 40, to indicate the importance of an event in which the wrong physical drive in an array set is replaced. The default is 12.
Event severity level for physical disk not responding	Set the event severity level from 1 to 40, to indicate the importance of an event in which a physical disk in an array set is not responding. The default is 12.
Event severity level for array enclosure overheating	Set the event severity level from 1 to 40, to indicate the importance of an event in which an array enclosure is overheating. The default is 12.
Event severity level for logical drive no longer functioning	Set the event severity level from 1 to 40, to indicate the importance of an event in which a logical drive in an array set is no longer functioning. The default is 5.
Event severity level for logical drive doing data expansion	Set the event severity level from 1 to 40, to indicate the importance of an event in which a logical drive in an array set is doing data expansion. The default is 15.

Description	How to Set It
Event severity level for logical drive ready for data expansion	Set the event severity level from 1 to 40, to indicate the importance of an event in which a logical drive in an array set is ready for data expansion. The default is 25.
Event severity level for logical drive unavailable	Set the event severity level from 1 to 40, to indicate the importance of an event in which a logical drive in an array set is unavailable. The default is 25.
Event severity level for unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of a logical drive in an array set is unknown. The default is 15.
Event severity level for unexpected Knowledge Script error	Set the event severity level from 1 to 40, to indicate the importance of an event in which the ArrayLogicalDriveStatus job fails unexpectedly. The default is 35.

ArrayPhysicalDiskStatus

Use this Knowledge Script to monitor the status of physical drives in an array set. This Knowledge Script raises an event if any physical drive is not operating or if any operation of the physical drive has degraded.

Resource Object

Array Physical Disk object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is n.
Event severity level for SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Event severity level for disk failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which a a physical drive in an array set fails. The default is 5.
Event severity level for disk degraded	Set the event severity level from 1 to 40, to indicate the importance of an event in which a physical drive in an array set is in a degraded condition. The default is 12.
Event severity level for unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of a physical drive in an array set is unknown. The default is 15.
Event severity level for unexpected Knowledge Script error	Set the event severity level from 1 to 40, to indicate the importance of an event in which the ArrayPhysicalDiskStatus job fails unexpectedly. The default is 35.

ASRHealth

Use this Knowledge Script to monitor Automatic Server Recovery (ASR) status. This Knowledge Script checks the overall condition of the ASR. The job raises an event if problems are detected. Event severity is specific to the failed condition.

This Knowledge Script also checks the number of ASR-initiated reboots that have occurred on a server during the monitoring interval. The job raises an event if the reboot count exceeds the threshold you set.

Resource Object

ASR object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for charts and reports. If set to **y**, the script returns the number of times ASR rebooted the system. The default is **n**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Reboot maximum threshold	Specify a threshold for the maximum number of server reboots before the job raises an event. The default is thrice.
Event severity level for SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Event severity level for overall condition critical	Set the event severity level from 1 to 40, to indicate the importance of an event in which the overall condition of the ASR is critical. The default is 2.
Event severity level for overall condition degraded	Set the event severity level from 1 to 40, to indicate the importance of an event in which the overall condition of the ASR is degraded. The default is 8.
Event severity level for number of reboots exceeded threshold	Set the event severity level from 1 to 40, to indicate the importance of an event in which the number of ASR-initiated reboots exceeded the threshold. The default is 5.

ASRStatus

Use this Knowledge Script to monitor changes to the Automatic Server Recovery (ASR) status. By default, the Knowledge Script checks the overall status of the ASR and the status of the Pager, DialIn, and DialOut functions. The job raises an event if the status of any monitored function changes during the monitoring interval.

Note
You can also raise an event when any ASR function is disabled. To have the Knowledge Script perform this check, set the Event severity level for ASR disabled parameter to a positive number.

Resource Object

ASR object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Check pager? (y/n)	Set to **y** to check Pager status. The default is **y**.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is **n**.
Check DialIn? (y/n	Set to **y** to check DialIn status The default is **y**.
Check DialOut? (y/n)	Set to **y** to check DialOut status. The default is **y**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Event severity level for SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Event severity level for ASR disabled	Set the event severity level from 1 to 40, to indicate the importance of an event in which the ASR is disabled. The default is -1.
Event severity level for ASR status change	Set the event severity level from 1 to 40, to indicate the importance of an event in which the ASR has a status change. The default is 8.

CorrectableMem

Use this Knowledge Script to monitor the condition of the correctable memory and the number of new correctable memory errors. The job raises an event if the number of correctable memory errors exceeds the threshold you set.

Resource Object

Correctable Memory object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for charts and reports. If set to **y**, the script returns the number of correctable memory errors. The default is **n**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Correctable memory errors maximum threshold	Specify a threshold for the maximum number of correctable memory errors. If you specify -1, the Knowledge Script uses the threshold value from a MIB variable inside SIM. **Note** Because the number of errors reported is a delta value for the interval, it is always 0 for the first interval.
Event severity level for SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Event severity level for overall condition critical	Set the event severity level from 1 to 40, to indicate the importance of an event in which the correctable memory has an overall condition of critical. The default is 2.
Event severity level for overall condition degraded	Set the event severity level from 1 to 40, to indicate the importance of an event in which the correctable memory has an overall condition of degraded. The default is 8.
Event severity level if correctable memory errors exceeded threshold	Set the event severity level from 1 to 40, to indicate the importance of an event in which the number of correctable memory errors exceeded the threshold. The default is 8.

CriticalErrorLog

Use this Knowledge Script to monitor the Critical Error Log for uncorrected critical error entries:

- A critical event indicates a failure entry in the Critical Error log.
- A degraded condition event indicates that an uncorrected error or degraded operation error has been recorded in the log.

Note
For more information about the raised events, check the entries using the Insight Manager Console.

Resource Object

Critical Error Log object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Failure entry	Set the event severity level from 1 to 40, to indicate the importance of an event in which a failure entry is recorded in the log. The default is 5.
Severity - Degraded condition entry	Set the event severity level from 1 to 40, to indicate the importance of an event in which an uncorrected error or degraded operation error has been recorded in the log. The default is 12.
Severity - Unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which a status of unknown is recorded in the log. The default is 15.

EventLog

Use this Knowledge Script to monitor the NT event log entries created by AppManager for HP SIM. These entries are in the System log. Insight Agents are listed as the source. You can define other parameters for filtering the event log, such as event category, event ID, user, server name, and description.

Resource Objects

SIM server objects

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for charts and reports. The default is **n**.
Start with events in past N hours	Set this parameter to determine which events are searched the first time you run the job. The following entries are valid: • **-1** to search all existing log entries during the first interval • **n** to search entries for the past *n* hours (8 for the past 8 hours, 50 for the past 50 hours, etc.) • **0** to search no previous entries (search from the current time forward) The default is 0.
Monitor for events of type: Error?	Set to **y** if you want to monitor Error events. The default is **y**.
Monitor for events of type: Warning?	Set to **y** if you want to monitor Warning events. The default is **y**.
Monitor for events of type: Information?	Set to **y** if you want to monitor Information events. The default is **n**.
Filter the Event Category field for	If you are interested in events in a particular category (for example 9 or 4), specify an appropriate search string. The Knowledge Script looks for matching entries in the Event Log's Category field. You can specify multiple strings separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter the Event ID field for	If you are interested in particular event IDs, specify an appropriate search string. The Knowledge Script looks for matching entries in the Event Log's Event field. You can specify multiple IDs separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.

Description	How to Set It
Filter the Event User field for	If you are interested in events associated with a particular user, specify an appropriate search string. The Knowledge Script looks for matching entries in the Event Log's User field. You can specify multiple strings separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter the Event Computer field for	If you are interested in events generated by a particular computer, specify an appropriate search string. The Knowledge Script looks for matching entries in the Event Log's Computer field. You can specify multiple strings separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter the Event Description field for	If you are interested in events with a particular detail description or containing keywords in the description, specify an appropriate search string. The Knowledge Script looks for matching entries in the Event Log's Description field. You can specify multiple strings separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Maximum number of log entries per event report	Specify the maximum number of log entries to be included in each event's detail message.The script returns multiple events if it finds more entries in the log than the maximum limit you specify. The default is 30 entries.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

FanIndividual

Use this Knowledge Script to monitor the status of individual fans. For each fan being monitored, this Knowledge Script raises an event if the fan is not operating properly or the status is unknown.

Resource Object

Fan object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Collect data?	Set to **y** to collect data for charts and reports. The default is **n**.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Critical condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which an individual fan is in critical condition. The default is 8.
Severity - Unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of an individual fan is unknown. The default is 15.

FanSummary

Use this Knowledge Script to monitor the status of System and CPU fans. When a required fan fails, this Knowledge Script raises an event indicating a critical condition. When a fan that is not required fails, this Knowledge Script raises an event indicating a degraded condition.

Resource Object

Fan object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is **n**.
Raise event if fan summary not supported (y/n)?	Set to **y** to raise an event if fan summary is not supported. The default is **n**.
Event severity level for SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Event severity level for critical failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which a required fan fails. The default is 8.
Event severity level for degraded condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which a fan that is not required fails. The default is 15.
Event severity level if fan summary not supported	Set the event severity level from 1 to 40, to indicate the importance of an event in which a fan summary is not supported. The default is 20.

FCAExternalControllerFail

Use this Knowledge Script to monitor the operational status of Fibre Channel Array external controllers.

The Knowledge Script raises:

- A critical event if the controller fails, making drives on the controller inaccessible.
- A degraded condition event if any of the controller's logical or physical drives is not operating properly.
- A warning if the status is not known.

Resource Object

FCA object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - Critical failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which a controller fails. The default is 5.
Severity - Degraded condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which any of the controller's logical or physical drives is not operating properly. The default is 12.
Severity - Unknown condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of a controller is unknown. The default is 15.

FCAFail

Use this Knowledge Script to monitor the status of Fibre Channel Array (FCA) controllers.

The Knowledge Script raises:

- A critical event if the controller fails, making drives on the controller inaccessible.
- A degraded condition event if any of the controller's logical or physical drives is not operating properly.
- A warning if the status is not known.

Resource Object

FCA object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Critical failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which the controller fails. The default is 5.
Severity - Degraded condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which any of the controller's logical or physical drives is not operating properly. The default is 12.
Severity - Unknown condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which the condition of the controller is unknown. The default is 9.

FCAHostControllerFail

Use this Knowledge Script to monitor the operational status of Fibre Channel host controllers.

The Knowledge Script raises:

- A critical event if the controller fails, making drives on the controller inaccessible.
- A degraded condition event if any of the controller's logical or physical drives is not operating properly.
- A warning if the status is not known.

Resource Object

FCA object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Critical failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which the controller fails, making drives on the controller inaccessible. The default is 5.
Severity - Degraded condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which any of the controller's logical or physical drives is not operating properly. The default is 12.
Severity - Unknown condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which the condition of the controller is unknown. The default is 15.

FCAHostFail

Use this Knowledge Script to monitor the status of Fibre Channel Array (FCA) host controllers.

The Knowledge Script raises:

- A critical event if the controller fails, making drives on the controller inaccessible.
- A degraded condition event if any of the controller's logical or physical drives is not operating properly.
- A warning if the status is not known.

Resource Object

FCA object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Controller failed	Set the event severity level from 1 to 40, to indicate the importance of an event in which the controller failed. The default is 5.
Severity - Degraded drive	Set the event severity level from 1 to 40, to indicate the importance of an event in which any of the controller's logical or physical drives is not operating properly. The default is 12.
Severity - Unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of the controller is unknown. The default is 15.

FCAOverallCondition

Use this Knowledge Script to monitor the overall condition of the FCA system.

The Knowledge Script raises:

- A critical event if the controller fails, making drives on the controller inaccessible.
- A degraded condition event if any of the host controller's logical or physical drives is not operating properly.
- A warning if the status is not known.

Resource Object

FCA object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Controller failed	Set the event severity level from 1 to 40, to indicate the importance of an event in which the controller fails. The default is 5.
Severity - Degraded drive	Set the event severity level from 1 to 40, to indicate the importance of an event in which any of the host controller's logical or physical drives is not operating properly. The default is 12.
Severity - Unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of a controller is unknown. The default is 15.

FLTPWRIndividualCondition

Use this Knowledge Script to monitor the status of fault tolerant power supplies. The job raises a critical or degraded operation event when the fault tolerant power supply is not operating properly.

Resource Object

Fault Tolerant Power Supply object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is **n**.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Power supply failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which a fault tower power supply fails. The default is 5.
Severity - Degraded operation	Set the event severity level from 1 to 40, to indicate the importance of an event in which an operation for a fault tolerant power supply is in a degraded condition. The default is 12.
Severity - Unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status if a fault tolerant power supply is unknown. The default is 15.

FLTPWROverallCondition

Use this Knowledge Script to monitor the overall condition of the fault tolerant power supply sub-system. The job raises a critical or degraded event when the sub-system is not operating properly.

Resource Object

Fault Tolerant Power Supply object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is **n**.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Power supply failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which the fault tolerant power supply sub-system fails. The default is 5.
Severity - Degraded operation	Set the event severity level from 1 to 40, to indicate the importance of an event in which an operation for a fault tolerant power supply sub-system is a degraded condition. The default is 12.
Severity - Unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of a fault tolerant power supply sub-system is unknown. The default is 15.
Severity - Unexpected Knowledge Script error	Set the event severity level from 1 to 40, to indicate the importance of and event in which the FLTPWROverallCondition Knowledge Script fails unexpectedly. The default is 35.

HealthCheck

Use this Knowledge Script to monitor all SIM services. The job raises an event if any service is not running and automatically re-starts the service. In addition, the `SNMP Get` function is explicitly exercised to ensure its proper operation. This Knowledge Script raises an event if the SNMP cannot get a SIM `MIB` variable.

Resource Object

SIM server services objects

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Auto-start service?	Set to **y** to automatically restart services that are down. The default is **y**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is **n**.
Severity - Service down; restart failed	Set the event severity level from 1 to 40, to indicate the importance of an event in which a SIM service is down and restart failed. The default is 5.
Severity - Service down; restart succeeded	Set the event severity level from 1 to 40, to indicate the importance of an event in which a SIM service was down and restart succeeded. The default is 25.
Severity - Service down; do not restart	Set the event severity level from 1 to 40, to indicate the importance of an event in which a SIM service is down and will not be restarted. The default is 18.
Severity - SNMP service down or cannot get MIB value.	Set the event severity level from 1 to 40, to indicate the importance of an event in which a SIM service is down or cannot get the MIB value. The default is 5.

IDAFail

Use this Knowledge Script to monitor IDA controllers.

The Knowledge Script raises:

- A critical event if an IDA drive fails.
- A degraded condition event if any IDA drive is not operating properly.
- A warning if the status is not known.

Resource Object

IDA

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the community name. The default is either the community name specified in the Security Manager or *public* if no community name has been specified.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is **n**.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Failed drive	Set the event severity level from 1 to 40, to indicate the importance of an event in which an IDA drive fails. The default is 5.
Severity - Degraded drive	Set the event severity level from 1 to 40, to indicate the importance of an event in which an IDA drive is not operating properly. The default is 12.
Severity - Unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of an IDA drive is unknown. The default is 15.

IDEFail

Use this Knowledge Script to monitor IDE controllers.

The Knowledge Script raises:

- A critical event if an IDE drive fails.
- A degraded condition event if any IDE drive is not operating properly.
- A warning if the status is not known.

Resource Object

IDE

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the community name. The default is either the community name specified in the Security Manager or *public* if no community name has been specified.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is **n**.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Failed drive	Set the event severity level from 1 to 40, to indicate the importance of an event in which an IDE drive fails. The default is 5.
Severity - Degraded drive	Set the event severity level from 1 to 40, to indicate the importance of an event in which an IDE drive is not operating properly. The default is 12.
Severity - Unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of an IDE drive is unknown. The default is 15.

IntegratedLog

Use this Knowledge Script to monitor the current status of the SIM log. The job raises an event if it is not able to scan the SIM log or if it finds unsupported Knowledge Scripts running on the SIM agent.

If this Knowledge Script cannot scan the SIM log, it returns, `"Failed to scan Integrated Management Log: errcode = "`. If an unsupported Knowledge Script is run on the SIM agent, it returns, `"This Knowledge Script is not supported on this Compaq server."`

Resource Object

Integrated management log

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is **y**.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is **n**.
Community	Specify the community name. The default is either the community name specified in the Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Component failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which a component fails. The default is 8.
Severity - Non-fatal error	Set the event severity level from 1 to 40, to indicate the importance of an event in which a non-fatal error occurs. The default is 15.
Severity - Informational but with LCD alert message	Set the event severity level from 1 to 40, to indicate the importance of an informational but with LCD alert message. The default is 20.
Ignore log entries without date and time?	Set to **y** to allow the IntegratedLog Knowledge Script job to ignore log entries for which there is no date or time. If set to n, the IntegratedLog Knowledge Script job monitors log entries for which there is no date or time. However, because the job cannot determine whether these entries are old or new, the job may return results for them more than once.

NICError

Use this Knowledge Script to monitor network interface transmission errors. Both input and output errors are reported and compared to respective thresholds. The job raises an event when the number of network interface errors per minute exceeds the threshold you set.

Resource Object

NIC object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for charts and reports. The default is **n**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Input errors per minute maximum threshold	Specify a threshold for the maximum number of input errors per minute. The default is 2 errors per minute.
Output errors per minute maximum threshold	Specify a threshold for the maximum number of output errors per minute. The default is 4 errors per minute.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Input errors per minute exceeded threshold	Set the event severity level from 1 to 40, to indicate the importance of an event in which input errors per minute exceeded the threshold you set. The default is 10.
Severity - Output errors per minute exceeded threshold	Set the event severity level from 1 to 40, to indicate the importance of an event in which output errors per minute exceeded the threshold you set. The default is 10.

NICFail

Use this Knowledge Script to monitor the status of the network interface. This Knowledge Script checks whether the network interface subsystem is down when the administrator has indicated it should be in the "up" state. The event details message includes the time when the interface was discovered as down.

Resource Object

NIC object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is **n**.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Interface down	Set the event severity level from 1 to 40, to indicate the importance of an event in which the network interface subsystem is down. The default is 6.

Report_ASRHealth-RebootCount

Use this CIM_Report script to generate a report about Automatic Server Recovery (ASR) status, and the number of ASR-initiated reboots. This report allows you to make a statistical analysis of the data point values over the time range you define for the report.

This report uses data collected by the ASRHealth Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Filter the data in your report by computer name.
Select time range	Filter the data in your report by a specific or sliding time range.
Select peak weekday(s)	Filter the data in your report by the days of the week.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the datastreams (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N% of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N% of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)

Description	How to Set It
Percentage/count for top/ bottom	Specify a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or percent (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is **yes**.
Include table?	Set to **yes** to include a table of datastream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of datastream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. The default is no. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Set miscellaneous report properties as required.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is **yes**.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Report_CIMResource_CPU_MemoryUsage

Use this CIM_Report script to generate a report about CPU and memory usage by SIM processes. This report allows you to make a statistical analysis of the data point values over the time range you define for the report.

This report uses data collected by the ResourceHigh Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Filter the data in your report by computer name.
Select time range	Filter the data in your report by a specific or sliding time range.
Select peak weekday(s)	Filter the data in your report by the days of the week.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the datastream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the datastream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N% of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N% of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or percent (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of datastream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of datastream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).

Description	How to Set It
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Report_CIMSCSI-Status

Use this CIM_Report script to generate a report about the number of hard resets, soft resets, and command timeouts for the SCSI controller. This report allows you to make a statistical analysis of the data point values over the time range you define for the report.

This report uses data collected by the SCSITimeout Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Filter the data in your report by computer name.
Select time range	Filter the data in your report by a specific or sliding time range.
Select peak weekday(s)	Filter the data in your report by the days of the week.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the datastream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the datastream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N% of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N% of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or percent (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of datastream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of datastream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).

Description	How to Set It
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Report_CorrectableMemoryErrors

Use this CIM_Report script to generate a report about the condition of correctable memory and the number of new correctable memory errors. This report allows you to make a statistical analysis of the data point values over the time range you define for the report.

This report uses data collected by the CorrectableMem Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Filter the data in your report by computer name.
Select time range	Filter the data in your report by a specific or sliding time range.
Select peak weekday(s)	Filter the data in your report by the days of the week.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the datastream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N% of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N% of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)

Description	How to Set It
Percentage/count for top/ bottom	Specify a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or percent (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of datastream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of datastream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Report_NewEventLogEntries

Use this CIM_Report script to generate a report about Windows event log entries with the SIM Insight Agent as the source. This report allows you to make a statistical analysis of the data point values over the time range you define for the report.

This report uses data collected by the EventLog Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Filter the data in your report by computer name.
Select time range	Filter the data in your report by a specific or sliding time range.
Select peak weekday(s)	Filter the data in your report by the days of the week.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the datastream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N% of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N% of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)

Description	How to Set It
Percentage/count for top/ bottom	Specify a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or percent (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of datastream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of datastream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Report_NICErrorRate

Use this CIM_Report script to generate a report about network interface input and output errors. This report allows you to make a statistical analysis of the data point values over the time period you define for the report.

This report uses data collected by the NICError Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Filter the data in your report by computer name.
Select time range	Filter the data in your report by a specific or sliding time range.
Select peak weekday(s)	Filter the data in your report by the days of the week.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the datastream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the datastream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N% of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N% of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or percent (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of datastream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of datastream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).

Description	How to Set It
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

ResourceHigh

Use this Knowledge Script to monitor the CPU and memory used by the SIM process. The job raises an event if the CPU or memory usage exceeds the threshold you set.

Resource Object

SIM server object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for charts and reports. The default is **n**.
%CPU usage maximum threshold	Specify a threshold for the maximum percentage of the CPU the SIM process should use. The default is 60%.
Memory usage maximum threshold	Specify a threshold for the maximum memory (in MB) the SIM process should use. The default is 6MB.
Event severity level	You can set the event severity level, from 1 to 40, to indicate the importance of this event. The default is 8.

RIBBatteryRechargeLevel

Use this Knowledge Script to monitor the battery recharge level of the Remote Insight Board. The job raises an event if the battery recharge level is below the threshold you set.

Resource Object

Remote Insight Board object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for charts and reports. The default is **n**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Recharge level minimum threshold	Specify a threshold for the minimum percentage to which the battery is recharged. The default is 75%.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Recharge level below threshold	Set the event severity level from 1 to 40, to indicate the importance of an event in which the battery recharge level of the Remote Insight Board is below the threshold you set. The default is 5.

RIBBatteryStatus

Use this Knowledge Script to monitor the status of the Remote Insight Board battery. The job raises an event if the battery has failed or is disconnected.

Resource Object

Remote Insight Board object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for charts and reports. The default is **n**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Battery failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which the Remote Insight Board battery fails. The default is 5.
Severity - Battery disconnected	Set the event severity level from 1 to 40, to indicate the importance of an event in which the Remote Insight Board battery **is disconnected**. The default is 15.
Severity - Unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of the Remote Insight Battery is unknown. The default is 15.

RIBCableConnections

Use this Knowledge Script to monitor the status of the Remote Insight board cable connections, including the keyboard, mouse, and external power cable. The job raises an event if any cable is disconnected.

Resource Object

Remote Insight Board object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is **n**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Cable disconnected	Set the event severity level from 1 to 40, to indicate the importance of an event in which a Remote Insight Board cable is disconnected. The default is 5.
Severity - Unknown connection status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of a Remote Insight Board connection is unknown. The default is 15.

RIBCondition

Use this Knowledge Script to monitor the overall condition of the Remote Insight Board. The job raises a failed or degraded event if the board is not operating properly.

Resource Object

Remote Insight Board object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for charts and reports. The default is **n**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Failed board	Set the event severity level from 1 to 40, to indicate the importance of an event in which the Remote Insight Board fails. The default is 5.
Severity - Degraded board	Set the event severity level from 1 to 40, to indicate the importance of an event in which the Remote Insight Board is not operating properly. The default is 8.
Severity - Unknown condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which the condition of the Remote Insight Board is unknown. The default is 15.

RIBInterfaceStatus

Use this Knowledge Script to monitor the interface status of the Remote Insight board. The job raises an event if the firmware of the board is not responding to commands.

Resource Object

Remote Insight Board object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for charts and reports. The default is **n**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Not responding	Set the event severity level from 1 to 40, to indicate the importance of an event in which the firmware of the Remote Insight Board is not responding to commands. The default is 5.
Severity - Unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of the interface is unknown. The default is 15.

RIBVirtualPowerCable

Use this Knowledge Script to monitor the virtual power cable connection of the Remote Insight board. The job raises an event if the cable is disconnected.

Resource Object

Remote Insight Board object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for charts and reports. The default is **n**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Cable disconnected	Set the event severity level from 1 to 40, to indicate the importance of an event in which the virtual power cable of the Remote Insight Board battery **is disconnected**. The default is 5.
Severity - Unknown connection status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of the virtual power cable connection of the Remote Insight Board battery **is unknown**. The default is 15.

SCSIFail

Use this Knowledge Script to monitor Small Computer System Interface (SCSI) drives.

This Knowledge Script raises:

- A critical event if a SCSI drive fails.
- A degraded condition event if any SCSI drive is not operating properly.
- A warning if the status is not known.

Resource Object

SCSI object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Failed drive	Set the event severity level from 1 to 40, to indicate the importance of an event in which an SCSI drive fails. The default is 5.
Severity - Degraded drive	Set the event severity level from 1 to 40, to indicate the importance of an event in which the SCSI drive is not operating properly. The default is 12.
Severity - Unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of the SCSI drive is unknown. The default is 15.

SCSITimeout

Use this Knowledge Script to monitor the number of hard resets, soft resets, and command timeouts for the Small Computer System Interface (SCSI) controller during the monitoring interval. The job raises an event if any threshold is exceeded.

Resource Object

SCSI object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for charts and reports. If set to **y**, the script returns the number of hard resets, soft resets, and command timeouts in the interval. The default is **n**.
Hard reset maximum threshold	Specify a threshold for the maximum number of hard resets. The default is 0 hard resets.
Soft reset maximum threshold	Specify a threshold for the maximum number of soft resets. The default is 2 soft resets.
Command timeout maximum threshold	Specify a threshold for the maximum number of command timeouts. The default is 10 timeouts.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Hard reset threshold exceeded	Set the event severity level from 1 to 40, to indicate the importance of an event in which the hard reset threshold for the SCSI controller is exceeded. The default is 5.
Severity - Soft reset threshold exceeded	Set the event severity level from 1 to 40, to indicate the importance of an event in which the soft reset threshold for the SCSI controller is exceeded. The default is 8.
Severity - Timeout threshold exceed	Set the event severity level from 1 to 40, to indicate the importance of an event in which the timeout threshold for the SCSI controller is exceeded. The default is 12.

TeamedNICCondition

Use this Knowledge Script to monitor the condition of Teamed Network Interface Cards (NIC). Teamed NICs run in parallel to increase link speed. The job raises an event when Teamed NIC is degraded or fails.

Resource Object

Teamed NIC object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or HP NIC Agent failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which the Teamed NIC fails. The default is 9
Severity - Degraded condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which the Teamed NIC is in a degraded condition. The default is 12.
Severity - Critical condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which the Teamed NIC is in critical condition. The default is 8.
Severity - Unknown condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which the condition of the Teamed NIC is unknown. The default is 15.

TempIndividual

Use this Knowledge Script to monitor the status of SIM temperature sensors. If the temperature sensors are operating out of normal range, this Knowledge Script raises a degraded condition event. If the temperature sensors indicate a critical condition, this Knowledge Script raises a critical condition event.

Resource Object

SIM temperature sensor object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for charts and reports. If set to **y**, the script returns the number of hard resets, soft resets, and command timeouts in the interval. The default is **n**.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Critical condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which the SIM temperature sensors are in critical condition. The default is 3.
Degraded condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which the SIM temperature sensors are in a degraded condition. The default is 8.
Severity - Unknown status	Set the event severity level from 1 to 40, to indicate the importance of an event in which the status of the SIM temperature sensors is unknown. The default is 15.
Severity - Unexpected Knowledge Script error	Set the event severity level from 1 to 40, to indicate the importance of and event in which the TempIndividual Knowledge Script fails unexpectedly. The default is 35.

ThermalStatus

Use this Knowledge Script to monitor the system's thermal environment and the status of the system's temperature sensors. If the overall condition of the system's thermal environment is abnormal or the temperature sensors are operating out of normal range, this Knowledge Script raises a degraded condition event. If the thermal environment or temperature sensors indicate a critical condition, this Knowledge Script raises a critical condition event.

Resource Object

Temperature objects

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Collect data?	Set to **y** to collect data for charts and reports. The default is **n**.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - Critical condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which the system's thermal environment or temperature sensors are in critical condition. The default is 3.
Severity - Degraded condition	Set the event severity level from 1 to 40, to indicate the importance of an event in which the system's thermal environment or temperature sensors are in a degraded condition. The default is 8.

UPSBatteryLow

Use this Knowledge Script to monitor the UPS battery life. The job raises an event when the battery life is below the threshold you set. Only run this Knowledge Script when the computer is not using AC power if you want to check the UPS battery.

Resource Object

UPS object

Default Schedule

The default interval for this script is **Every 3 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Battery life minimum threshold	Specify a threshold for the minimum number of minutes of remaining battery life. The default is 3 minutes.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - AC power is on	Set the event severity level from 1 to 40, to indicate the importance of an event in which the AC power is on. The default is 25.
Severity - Battery is low	Set the event severity level from 1 to 40, to indicate the importance of an event in which the UPS battery life is below the threshold you set. The default is 2.

UPSLineStatus

Use this Knowledge Script to monitor the UPS AC power line. The job raises a critical event if the AC power line is down.

Resource Object

UPS object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Community	Specify the SNMP community string. The default is either the community name specified in AppManager Security Manager or *public* if no community name has been specified.
Severity - SNMP or CIM failure	Set the event severity level from 1 to 40, to indicate the importance of an event in which SNMP or HP SIM fails. The default is 9.
Severity - AC power line down	Set the event severity level from 1 to 40, to indicate the importance of an event in which the UPS AC power line is down. The default is 2.

Chapter 39
IBM Systems Director Knowledge Scripts

AppManager for IBM Systems Director provides the following Knowledge Scripts: for monitoring IBM Systems Director resources. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press F1.

Knowledge Script	What It Does
EventLog	Scans the Application log for IBM Systems Director entries.
FanSpeed	Monitors the speed of some or all fans on an IBM Systems Director server.
HealthCheckHW	Monitors the overall health of IBM Systems Director hardware components.
HealthCheckMgmtSrv	Monitors IBM Systems Director-related services.
MemoryErrors	Monitors the memory bank errors on an IBM Systems Director system.
NICError	Monitors the network interface controllers on an IBM Systems Director server for transmission errors.
ServeRAIDControllerStat	Monitors the operational status of ServeRAID controllers.
ServeRAIDLogicalDriveStat	Monitors the operational status of ServeRAID logical drives.
ServeRAIDPhysicalDrivePFA	Monitors for predicted failures of RAID physical drives.
ServeRAIDPhysicalDriveStat	Monitors the operational status of ServeRAID physical drives.
Temperature	Monitors the temperature on a IBM Systems Director server.
Voltage	Monitors the voltage levels on a IBM Systems Director server.
Discovery_NetfinityDir	Discovers IBM Systems Director configuration and resources.

EventLog

Use this Knowledge Script to scan the Application log for entries created by IBM Systems Director server.

In the first interval, the value you specify for the *Start with events in past N hours* option determines how far back in the log to check for matching entries. As the script continues to run at subsequent intervals, it checks for any new entries since the last log check.

You can further restrict the types of log entries that generate an event in two ways:

- Use the *Monitor for events of type* options to search only certain types of events, such as Warning events.
- Use the *Filter the [...] field for* options to search only for specific information, such as events with a specific ID.

Each time this script runs, it checks the Application log for entries matching your selection criteria and raises an event if matching entries are found. The event detail message returns the text of the log entries found. When this script is set to collect data, it returns the number of log entries found, and the data point detail message returns the text of the log entries.

Resource Object

Netfinity Director

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when the event log contains entries that match the criteria you specify. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this script returns the number of new event log entries matching your selection criteria. The detail message returns the text of the log entries. The default is n.
Start with events in past N hours	Set this option to determine which existing entries in the System log are scanned when the script starts to run: • **-1** scan all existing entries • **0** do not scan existing entries • **N** scan entries created in the past *N* hours (for example, 8 for the past 8 hours) The default is 0.
Monitor for Error events?	Set to **y** to monitor the event log for Error events. The default is y.
Monitor for Warning events?	Set to **y** to monitor the event log for Warning events. The default is y.
Monitor for Information events?	Set to **y** to monitor the event log for Information events. The default is y.

Description	How to Set It
Filter the Event ID field for	To monitor for particular Event IDs, enter an appropriate search string. The script looks for matching entries in the Event Log's Event field. Multiple IDs and ranges can be entered separated by commas. For example: 1,2,10-15,202. The search string can contain criteria used to include entries, exclude entries, or both. Separate include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter the Event Description field for	To monitor for events with a particular detail description or containing keywords in the description, enter an appropriate search string. The looks for matching entries in the Event Log's Description field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Maximum number of entries per event message	Specify the maximum number of entries to be recorded into each event's detail message. If the script finds more matching entries in the log than can be put into a single event message, it raises multiple events to return all the log entries. The default is 30 entries.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the event log contains entries that match your selection criteria. The default is 8.

FanSpeed

Use this Knowledge Script to monitor the speed of a particular fan or all fans on an IBM Systems Director server. This script is useful for collecting data on all fans on an IBM Systems Director server. To raise events on the overall health of an IBM Systems Director system, including fan speed-related events, use the HealthCheckHW Knowledge Script.

IBM Systems Director defines the upper and lower operating thresholds for fan speed. Use the IBM Systems Director-specified threshold values to monitor all fans or a particular fan and raise a Warning event when the fan speed is less than the upper threshold and a Critical event when the fan speed is less than the lower threshold. You can also set a parameter to raise an event if the fan speed is normal.

Alternatively, this script allows you to specify custom values for upper and lower thresholds. Check your IBM Systems Director documentation to determine the minimum speed for a fan and set the custom thresholds in this Knowledge Script accordingly. When using this script to raise events based on a custom threshold, to avoid raising false events on fans that run normally at different speeds, run the script on a particular fan sensor.

Resource Objects

Fan folder or a fan icon on a Netfinity Director server

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when fan speed exceeds the threshold you specify. The default is y.
Raise event when fan speed is normal?	Set to **y** to raise an event when fan speed is normal. The default is n.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, data collection records fan speed information for each fan you are monitoring. The default is n.
Threshold option (0 for standard, 1 for custom)	Specify a threshold option for raising events. Enter: • **0** to use the IBM Systems Director-specified threshold values for normal operation. Based on these threshold values, this Knowledge Script can raise a Warning event when the fan speed is below the upper threshold and a Critical event when the fan speed is below the lower threshold. • **1** to specify custom threshold values for the fan speed thresholds. The default is 0.
Custom threshold for a Warning event	Specify an upper threshold, in revolutions per minute, for raising a Warning event. For example, to raise a Warning event when the fan speed is less than 1,300 RPM, specify `1300`. The default is 750 RPM. To use this option, the *Threshold option* must be configured to raise an event based on custom thresholds (option 1).

Description	How to Set It
Custom threshold for a Critical event	Specify a lower threshold, in revolutions per minute, for raising a Critical event. For example, to raise a Critical event when the fan speed is less than 1,100 RPM, specify `1100`. The default is 500 RPM. To use this option, the *Threshold option* must be configured to raise an event based on custom thresholds (option 1).
Event severity levels...	Set the event severity level, from 1 to 40, to indicate the importance of the following events: • **...Normal event**. Fan speed is normal. The default is 30. • **...Warning event**. Fan speed is lower than the upper threshold. The default is 15. • **...Critical event.** Fan speed is lower than the lower threshold. The default is 5. • **...Threshold information is not available.** This can occur when the IBM Systems Director threshold or a custom threshold is 0. The default is 25.

HealthCheckHW

Use this Knowledge Script to monitor the current health information and predictive health information of IBM Systems Director hardware components, including voltage level, temperature, fan speed, and logical disk errors. This script raises an event when the status of a server component is considered by IBM Systems Director to be in a Warning or Critical state.

IBM Systems Director defines the operating thresholds for these components. You can use the default event severity levels for Warning and Critical events or set your own.

This script is useful for monitoring all of the voltage, temperature and fan sensors, and logical disks on an IBM Systems Director server.

Resource Object

Netfinity Director server

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when a server component is in Warning or Critical state. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, data collection records the overall status of voltage levels, temperature, fan speed, and logical disk errors. The default is n.
Event severity levels...	Set the event severity level, from 1 to 40, to indicate the importance of the following events: • **...Warning event.** The default is 15. • **...Critical event.** The default is 5.

HealthCheckMgmtSrv

Use this Knowledge Script to monitor the up and down status of IBM Systems Director-related services. If a service is not running, an event is raised and the service can be automatically restarted.

This script is useful for monitoring some or all of the IBM Systems Director-related services on an IBM Systems Director server.

Resource Object

Netfinity Director server

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Auto-start a service?	Set to **y** to automatically restart down services. The default is y.
Collect data?	Set to **y** to collect data for service status. If set to y, data collection records the service availability. The default is n.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...Failed to restart**. The default is 5. • **...Successful restart**. The default is 25. • **...Do not restart**. The default is 18.

MemoryErrors

Use this Knowledge Script to monitor the memory errors of an IBM Systems Director server. You can monitor the errors of an individual memory bank or all the memory banks of an IBM Systems Director system. An event is raised if the number of bits of memory errors exceeds the threshold.

Resource Objects

Physical Memory or a DIMM icon on a Netfinity Director server

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for memory bank errors. If set to y, data collection records the memory bank errors with the details of the memory slot. The default is n.
Threshold level	Specify the maximum amount of memory errors that can occur before an event is raised. The default is 1 bit.
Event severity levels...	Set the event severity level, from 1 to 40, to indicate the importance of the following events: • **...Critical event.** The default is 5. • **...Severity normal.** The default is 25.

NICError

Use this Knowledge Script to monitor the number of network interface controller (NIC) transmission errors on an IBM Systems Director server. Both input and output errors are reported and compared to respective thresholds. By default, if the number of NIC errors per minute exceeds the threshold you set, an event is raised.

This script is useful for collecting data and raising events on some or all NICs on an IBM Systems Director server.

Resource Objects

NIC folder NIC icon on a Netfinity Director server

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, data collection records the number of input and output errors per minute at each monitoring interval. The default is n.
Maximum threshold for input errors	Specify the maximum number of input errors that can occur per minuted before an event is raised. The default is 2 errors per minute.
Maximum threshold for output errors	Specify the maximum number of output errors that can occur per minute before an event is raised. The default is 4 errors per minute.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...input errors per minute exceed the threshold**. The default is 10. • **...output errors per minute exceed the threshold**. The default is 10.

ServeRAIDControllerStat

Use this Knowledge Script to monitor the operational status of ServeRAID controllers. If the RAID controller has failed or its status cannot be determined, an event is raised.

Note
This Knowledge Script attempts to query the metrics using SNMP, and if that fails, it uses WMI. An event is raised if both attempts fail.

Resource Object

RAID controller

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the RAID controller has failed or its status cannot be determined. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the RAID controller is functioning properly • **0** if the RAID controller has failed or the state cannot be determined The default is n.
Community	Provide the SNMP community name of the RAID device. The default is either the community name entered in AppManager Security Manager or *public* if no community name has been entered.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...SNMP and WMI, or IBM Director Agent failure**. The default is 9. • **...critical condition**. The default is 8. • **...unknown status**. The default is 15.

ServeRAIDLogicalDriveStat

Use this Knowledge Script to monitor the operational status of ServeRAID logical drives. If the RAID logical drive is offline, migrating, free, or in critical condition or unknown state, an event is raised.

Note
This Knowledge Script attempts to query the metrics using SNMP, and if that fails, it uses WMI. An event is raised if both attempts fail.

Resource Objects

RAID logical drives

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the RAID logical drive is offline, migrating, free, or in a critical or unknown state. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the RAID logical drive is functioning properly • **50** if the RAID logical drive is offline, migrating, free, or degraded • **0** if the RAID logical drive is in critical condition or the state cannot be determined The default is n.
Community	Provide the SNMP community name of the RAID device. The default is either the community name entered in AppManager Security Manager or *public* if no community name has been entered.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...SNMP and WMI, or IBM Director Agent failure**. The default is 9. • **...critical condition**. The default is 8. • **...drive offline, migrating, or free**. The default is 18. • **...unknown status**. The default is 15.

ServeRAIDPhysicalDrivePFA

Use this Knowledge Script to monitor for predicted failures of RAID physical drives. If a failure is predicted, an event is raised.

Note
This Knowledge Script attempts to query the metrics using SNMP, and if that fails, it uses WMI. An event is raised if both attempts fail.

Resource Objects

RAID disk drives

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a failure is predicted for the RAID physical drive. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the RAID physical drive is functioning properly • **0** if a failure is predicted for the RAID physical drive The default is n.
Community	Provide the SNMP community name of the RAID device. The default is either the community name entered in AppManager Security Manager or *public* if no community name has been entered.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...SNMP and WMI, or IBM Director Agent failure**. The default is 9. • **...failure predicted**. The default is 8.

ServeRAIDPhysicalDriveStat

Use this Knowledge Script to monitor the operational status of ServeRAID physical drives. If the RAID physical drive is ready, on standby, being rebuilt, not present, or in an unknown state, an event is raised.

Note
This Knowledge Script attempts to query the metrics using SNMP, and if that fails, it uses WMI. An event is raised if both attempts fail.

Resource Objects

RAID disk drives

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a RAID physical drive is ready, on standby, being rebuilt, not present, or in an unknown state. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the RAID physical drive is online, or is a spare drive • **50** if the RAID physical drive is ready, on standby, or being rebuilt • **0** if the RAID physical drive is down, not present, or the state cannot be determined The default is n.
Community	Provide the SNMP community name of the RAID device. The default is either the community name entered in AppManager Security Manager or *public* if no community name has been entered.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...SNMP and WMI, or IBM Director Agent failure**. The default is 9. • **...drive is down**. The default is 8. • **...drive on standby, being rebuilt, or ready**. The default is 18. • **...unknown status**. The default is 15.

Temperature

Use this Knowledge Script to monitor a particular temperature sensor or all temperature sensors on an IBM Systems Director server. This script is useful for collecting data on all temperature sensors on an IBM Systems Director server. To raise events on the overall health of an IBM Systems Director system, including temperature-related events, use the HealthCheckHW Knowledge Script.

IBM Systems Director defines the lower and upper operating thresholds for temperature. Use the IBM Systems Director-specified threshold values to monitor all temperature sensors or a particular temperature sensor and raise a Warning event when the temperature is higher than the lower threshold and a Critical event when the temperature is higher than the upper threshold.

Alternatively, this script allows you to specify custom values for lower and upper thresholds. Check your IBM Systems Director documentation to determine an acceptable lower and upper threshold for temperature and set the custom thresholds in this script accordingly. When using this script to raise events based on a custom threshold, to avoid raising false events on temperature sensors that run normally at different temperatures, run the script on a particular temperature sensor.

Resource Objects

Temperature folder or a temperature icon on a Netfinity Director server

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a value exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the temperature detected by the sensor in Celsius. The default is n.
Threshold option (0 for standard, 1 for custom)	Specify a threshold for raising events. Enter: • **0** to use the IBM Systems Director-specified threshold values for normal operation. Based on these thresholds, this Knowledge Script can raise a Warning event when the temperature is above the lower threshold and a Critical event when the temperature is above the upper threshold. • **1** to specify custom threshold values for lower and upper temperature thresholds. The default is 0.
Custom threshold for a Warning event	Specify a lower threshold, in Celsius, for raising a Warning event. For example, to raise a Warning event when the operating temperature is higher than 60° Celsius, specify `60`. The default is 65° Celsius. To use this option, the *Threshold option* must be configured to raise an event based on custom thresholds (option 1).

Description	How to Set It
Custom threshold for a Critical event	Specify an upper threshold, in Celsius, for raising a Critical event. For example, to raise a Critical event when the operating temperature is higher than 85° Celsius, specify 85. The default is 80° Celsius. To use this option, the *Threshold option* must be configured to raise an event based on custom thresholds (option 1).
Event severity levels...	Set the event severity level, from 1 to 40, to indicate the importance of the following events: • **...Warning event.** Temperature is above the lower threshold. The default is 15. • **...Critical event**. Temperature is above the upper threshold. The default is 5. • **...Threshold information is not available**. This can occur when the IBM Systems Director threshold or a custom threshold is 0. The default is 25.

Voltage

Use this Knowledge Script to monitor the voltage levels for a particular voltage sensor or all voltage sensors on an IBM Systems Director server. To raise events on the overall health of an IBM Systems Director system, including voltage-related events, use the HealthCheckHW Knowledge Script.

IBM Systems Director defines the operating range for voltage sensors. Use this script to monitor all voltage sensors or a particular voltage sensor and raise an event when the voltage level is above the upper threshold or below the lower threshold specified by IBM Systems Director. You can also set a parameter to raise an event when the voltage level is normal.

Resource Objects

Voltage folder or a voltage icon on a Netfinity Director server

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a value exceeds or falls below the threshold. The default is y.
Raise an event when the voltage level is normal?	Set to **y** to raise an event when the voltage level is normal. The default is n.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the voltage level detected by each sensor you monitor. The default is n.
Event severity levels...	Set the event severity level, from 1 to 40, to indicate the importance of the following events: • **...Voltage level is normal**. Voltage level is normal. The default is 30. • **...Low level threshold**. Voltage level is below the lower threshold. The default is 5. • **...High level threshold**. Voltage level is above the upper threshold. The default is 5. • **...Threshold information is not available**. This can occur when the IBM Systems Director threshold is 0. The default is 25.

Discovery_NetfinityDir

Use this Knowledge Script to discover the resource and configuration information of IBM Systems Director.

When the discovery process completes successfully, IBM Systems Director Knowledge Scripts appear in the **Netfinity** view of the Operator Console in the NetfinityDir tab of the Knowledge Script pane.

Resource Objects

IBM Systems Director servers

Default Schedule

By default, this script is only run once for each computer.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event for successful discovery?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to y to raise an event when the job succeeds. The default is n.
SNMP community string	Provide the SNMP community name of the IBM Systems Director server. The default is either the community name entered in AppManager Security Manager or *public* if no community name has been entered.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25. • **...is partially done**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 15. • **...fails**. The default is 5. **Note** If required services, such as SNMP and WMI, are not running on the computer you are discovering, you may see a severity 15 event. If you see this type of event, see the detail message for more information about what caused the discovery to fail.

Chapter 40
IIS Knowledge Scripts

In addition to Knowledge Scripts for monitoring IIS performance and availability, AppManager for IIS also provides many IIS-specific Knowledge Scripts to generate reports for IIS information.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

The IIS category provides the following Knowledge Scripts for monitoring Microsoft Internet Information Services resources.

Knowledge Script	What It Does
ApplicationPools	Monitors application pools.
ASPCommFailure	Monitors the number of communication failures during an interval.
ASPEventLog	Monitors and filters ASP and ASP.NET information in the Windows Application Event Log.
ASPNETApplicationRestarted	Monitors the number of ASP.NET application restarts during a monitoring interval.
ASPNETApplicationRunning	Monitors the number of running ASP.NET applications during a monitoring interval.
ASPNETErrors	Monitors the total number of ASP.NET errors during the monitoring interval.
ASPNETPipelineInstances	Monitors the number of ASP.NET pipeline instances during a monitoring interval.
ASPNETReqStat	Monitors: • Number of current ASP.NET requests • Number of ASP.NET requests disconnected • Time taken to execute ASP.NET requests • Number of queued ASP.NET requests • ASP.NET request processing rate • Number of ASP.NET requests rejected • Wait time before processing the most recent ASP.NET request
ASPNETRequestCurrent	Monitors the number of current ASP.NET requests.
ASPNETRequestDisconnected	Monitors the number of ASP.NET requests from clients that disconnected during a monitoring interval.
ASPNETRequestExecuteTime	Monitors the time the most recent ASP.NET request required to execute.

Knowledge Script	What It Does
ASPNETRequestQueued	Monitors the number of ASP.NET requests that are queued to be serviced.
ASPNETRequestRate	Monitors the ASP.NET request processing rate.
ASPNETRequestRejected	Monitors the number of ASP.NET requests that were rejected during a monitoring interval.
ASPNETRequestWaitTime	Monitors the time the most recent ASP.NET request waited to be serviced.
ASPNETWorkerProcessCPU	Monitors the CPU usage of the ASP.NET worker processes during a monitoring interval.
ASPNETWorkerProcessExcepRate	Monitors the current exception rate for the common language runtime (CLR) in all ASP.NET worker processes.
ASPNETWorkerProcessExceptions	Monitors the number of CLR exceptions thrown in all ASP.NET worker processes during a monitoring interval.
ASPNETWorkerProcessMemory	Monitors the nonshared memory (private) usage of the ASP.NET worker processes during a monitoring interval.
ASPNETWorkerProcessRestarted	Monitors the number of ASP.NET worker process restarts during a monitoring interval.
ASPNETWorkerProcessRunning	Monitors the number of running ASP.NET worker processes during a monitoring interval.
ASPQueueBusy	Monitors the number of ASP requests currently in the queue.
ASPRegistryChange	Monitors changes to registry keys or values.
ASPReqStat	Monitors: • Number of ASP request errors • Different types of ASP request failures • ASP sessions that timed out.
ASPRequestError	Monitors the number of ASP request errors per second.
ASPRequestFailed	Monitors the number of different types of ASP request failures during an interval.
ASPSessionTimeout	Monitors the number of ASP sessions that timed out during an interval.
ASPThroughput	Monitors the throughput rate for ASP requests.
CacheHitRatio	Monitors the cache hit ratio for cache requests during the monitoring interval.
CentralizedBinaryLogging	Extracts information from the IIS centralized binary logging file.
CGIRequests	Monitors the CGI requests for a Web site during the monitoring interval.
CpuHigh	Monitors the CPU usage of specified IIS application processes.
FTPBytes	Monitors the rate of bytes transferred per second to and from the FTP server.
FTPConnections	Monitors the current number of connections to FTP sites.
FTPConnectionsInterval	Monitors the number of FTP site connections from anonymous and user accounts over the monitoring interval.
FTPConnectionUtil	Monitors the percentage of FTP connections being utilized.

Knowledge Script	What It Does
FTPFiles	Monitors the total number of files sent to and received from the FTP server.
FTPStatistics	Monitors: • Current number of connections to FTP sites • Number of FTP site connections • Percentage of FTP connections being utilized.
FTPTransStat	Monitors the rate of bytes transferred per second and the total number of files sent to and received from the FTP server.
HealthCheck	Checks whether any IIS services or Web sites are down and tracks queue length for blocked I/O requests.
HTTPBytes	Monitors the total number of bytes transferred per second to and from a Web site.
HTTPBytesInterval	Monitors the total number of bytes transferred to and from Web sites during a monitoring interval.
HTTPConnectionsInterval	Monitors the number of HTTP connections during a monitoring interval.
HTTPConnectionUtil	Monitors the percentage of Web site connections being utilized.
HTTPFiles	Reports the total number of files sent to and received from the Web server during a monitoring interval.
HTTPNotFound	Reports the number of requested pages that could not be found by the Web server during a monitoring interval.
HTTPRequests	Monitors the total number of HTTP method requests.
HTTPStatistics	Monitors: • Current number of HTTP connections to a Web site • Number of HTTP connections • Percentage of Web server connections being utilized.
HTTPTransStat	Monitors the total number of bytes transferred per second and the number of bytes transferred to and from Web sites, during a monitoring interval.
IsolatedApps	Monitors the number of isolated applications within a Web site.
KillTopCPUProcs	Monitors the CPU usage for IIS processes (`w3wp` for IIS 6.0).
Log	Monitors and filters information in the IIS Web site logs.
MemoryHigh	Monitors the memory usage of specified IIS application processes.
NNTPArticles	Monitors the number of articles processed by the NNTP server.
NNTPBytes	Monitors the number of bytes processed by the NNTP server.
NNTPClientCommands	Monitors the number of client requests processed by the NNTP server.
NNTPClientFailures	Monitors the number of client security request failures processed by the NNTP server.
NNTPConnections	Monitors the current number of connections to the NNTP server.
NNTPConnectionsInterval	Monitors the of inbound and outbound connections to the NNTP server during a monitoring interval.
NNTPConnectionUtil	Monitors the percentage of NNTP server connections being utilized.

Knowledge Script	What It Does
NNTPEventLog	Monitors and filters information in the Event Log.
NNTPServerFailures	Monitors the number of NNTP server failures that occurred in the specified interval.
NNTPSpaceLow	Monitors used and free disk space on each drive serving as an NNTP virtual root.
NNTPStatistics	Monitors: • Current number of connections to NNTP server • Inbound and outbound connections to the NNTP server • Percentage of NNTP connections being utilized.
Report_ASPCommunicationFailure	Generates a report about the number of ASP communication failures.
Report_ASPNETApplicationRestarted	Generates a report about the number of ASP.NET application restarts.
Report_ASPNETApplicationRunning	Generates a report about the number of ASP.NET applications running.
Report_ASPNETErrors	Generates a report about the number of ASP.NET application errors.
Report_ASPNETPipelineInstances	Generates a report about the number of ASP.NET pipeline instances.
Report_ASPNETReqStat	Generates a report about the number of: • ASP.NET current requests • Disconnected ASP.NET requests • ASP.NET request execution time • Queued ASP.NET requests • ASP.NET requests processed per second • Rejected ASP.NET requests • Wait time of ASP.NET requests.
Report_ASPNETRequestCurrent	Generates a report about the number of ASP.NET current requests.
Report_ASPNETRequestDisconnected	Generates a report about the number of ASP.NET requests from clients that disconnected.
Report_ASPNETRequestExecuteTime	Generates a report about the execution time for ASP.NET requests.
Report_ASPNETRequestQueued	Generates a report about the number of ASP.NET requests queued.
Report_ASPNETRequestRate	Generates a report about the ASP.NET request rate.
Report_ASPNETRequestRejected	Generates a report about the number of ASP.NET requests rejected.
Report_ASPNETRequestWaitTime	Generates a report about the average ASP.NET request wait time.
Report_ASPNETWorkerProcessCPU	Generates a report about the CPU utilization of ASP.NET worker processes.
Report_ASPNETWorkerProcessExcepRate	Generates a report about the number of CLR exceptions thrown per second in all ASP.NET worker processes.
Report_ASPNETWorkerProcessExceptions	Generates a report about the number of CLR exceptions thrown in all ASP.NET worker processes.

Knowledge Script	What It Does
Report_ASPNETWorkerProcessMemory	Generates a report about ASP.NET memory usage.
Report_ASPNETWorkerProcessRestarted	Generates a report about the number of ASP.NET worker processes that were restarted.
Report_ASPNETWorkerProcessRunning	Generates a report about the number of ASP.NET worker processes that were running.
Report_ASPNewEventLogEntries	Generates a report about the number of ASP events.
Report_ASPQueueBusy	Generates a report about the number of ASP requests currently in the queue.
Report_ASPRegistryChange	Generates a report about the number of changes to ASP registry keys.
Report_ASPReqStat	Generates a report about the number of: • ASP request errors • Different types of ASP request failures • ASP sessions that timed out
Report_ASPRequestError	Generates a report about the number of ASP request errors per second.
Report_ASPRequestFailed	Generates a report about the number of ASP request failures by error type.
Report_ASPSessionTimeout	Generates a report about the number of ASP sessions that timed out during an interval.
Report_ASPThroughput	Generates a report about the number of ASP requests processed per second.
Report_CpuUsage	Generates a report about the CPU usage of IIS application processes.
Report_FTPBytesRate	Generates a report about the total number of bytes transferred per second to and from an FTP site.
Report_FTPConnections	Generates a report about the current number of connections from anonymous and user accounts to an FTP site.
Report_FTPFilesTransferRate	Generates a report about the total number of files sent to and received from an FTP server during the monitoring interval.
Report_FTPTransStat	Generates a report about the total number of bytes transferred and the total number of files sent to and received from the FTP server.
Report_HTTPC21WebTransferRate	Generates a report about the total number of bytes transferred per second to and from a Web server.
Report_HTTPNotFoundError	Generates a report about the number of requested pages that could not be found by the Web server per monitoring interval.
Report_MemoryUsage	Generates a report about the number of bytes of memory being used by the specified IIS process.
Report_NNTPArticlesTransferRate	Generates a report about the current number of articles processed by the NNTP server.
Report_NNTPBytesTransferRate	Generates a report about the current number of bytes processed by the NNTP server.
Report_NNTPClientCommands	Generates a report about the number of client commands processed by the NNTP server.

Knowledge Script	What It Does
Report_NNTPClientFailures	Generates a report about the number of client security request failures processed by the NNTP server.
Report_NNTPCurrentConnections	Generates a report about the total number of connections to the NNTP server.
Report_NNTPTransStat	Generates a report about the number of articles and bytes processed by the NNTP server.
Report_NNTPVirtualRootDiskSpace	Generates a report about the used and free disk space for each drive that is used as an NNTP virtual root.
RestartServer	Restarts an IIS server.
ServiceUptime	Monitors the uptime for Web sites and services, and FTP sites and services.
SMTPBytesInterval	Monitors the total number of bytes transferred to and from SMTP sites during a monitoring interval.
SMTPConnections	Monitors the number of current inbound and outbound connections on an SMTP site, and outbound connection attempts refused by remote sites.
SMTPConnectionsInterval	Monitors the number of inbound and outbound connections to and from SMTP sites during the monitoring interval.
SMTPConnectionUtil	Monitors the percentage of SMTP site connections being utilized.
SMTPMsgs	Monitors SMTP messages for the total number of bytes sent and received, messages delivered, inbound messages received, and outbound messages sent during a monitoring interval.
SMTPQueue	Monitors the number of messages in the local, remote, local retry, and remote retry queues.
SMTPStatistics	Monitors: • Number of current connections on an SMTP site • Inbound and outbound connections to and from the SMTP site • Percentage of SMTP connections being utilized
SSLCertMon	Identifies and monitors the status of SSL certificates on the Web server.
UDDIConnections	Monitors Web servers running the UDDI services database and UDDI directory.
UnloadApps	Unloads applications from a Web server.
WebServiceExtensions	Extracts the IIS Web service extensions and their status.

ApplicationPools

Use this Knowledge Script to monitor the health, performance, and recycling properties of application pools. An application pool is a set of isolated Web applications hosted on a common server. Each application pool is allocated a set of server resources.

For example, if a Web site with a memory leak is in an independent application pool, it does not affect any other Web site because each application pool has its own server resources (including memory). If the application pool data collection fails or succeeds, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Start application pools if stopped?	Select **Yes** to start the application pools. The default is No.
Collect data of application pool health properties?	Select **Yes** to collect data for charts and reports. By default, data is collected.
Event severity when application pool fails to start or data collection fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity when application pool starts or data collection succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

ASPCommFailure

Use this Knowledge Script to monitor the number of ASP communication failures during a monitoring interval. This Knowledge Script considers requests disconnected as communication failures. If the number of ASP communication failures exceeds the threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Note
If the schedule is set to Run Once, the value returned is the current total, not the total for the monitoring interval.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of failures exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for ASP communication failures?	Set to **y** to collect data for charts and reports. If set to y, the script returns both the number of failures and the failure rate. The default is n.
Threshold -- Maximum number of ASP communication failures	Specify the maximum number of communication failures allowed before AppManager raises an event. The default is 25 failures.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

ASPEventLog

Use this Knowledge Script to monitor the Windows Application Event Log for entries in the Application Event Log that have Active Server Pages as their Source and ASP.NET events.

During the first monitoring interval, the value you specify for the **Starting point for log search (past N hours)** parameter determines how far back in the log to check for matching entries. As the script continues to run at subsequent intervals, it checks for any new entries created since the last time the log was checked.

You can further restrict the types of log entries that generate an event in two ways:

- Use the **Event type [...]** parameters to search only certain types of events, such as Warning events.
- Use the **Filter [...]** parameters to search only for specific information, such as events associated with a specific user or computer name.

Each time this Knowledge Script runs, it checks the Event Log for entries matching your selection criteria and raises an event if matching entries are found. The event detail message returns the text of the log entries found. When this Knowledge Script is set to collect data, it returns the number of log entries found, and the data point detail message returns the text of the log entries.

When you search for ASP or ASP.NET events, the script populates the event log with matching data. This includes the search result along with the version number. For example, if you select ASP.NET as the search criterion, the result displays ASP.NET v1.1.4322, where "v1.1.4322" is the version number of ASP.NET.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if log entries match search criteria?	Set to **y** to raise an event if the log entries match the search criteria. The default is y.
Filters the event log for counter:	Select to filter the event log. The default is Active Server Pages.
Collect data for matching log entries?	Set to **y** to collect data for charts and reports. If set to y, returns the number of matching Event Log entries, and the detailed message lists the log entries. The default is n.

Description	How to Set It
Starting point for log search (past *N* hours)	Set this parameter to determine which events to search for the **first** time the Knowledge Script is run. Subsequent searches begin where the last search finished. The following values are valid: • **-1**: Search all Event Log events that occurred before and during the first monitoring interval. • **0**: Search only for events that occurred during the monitoring interval; previous events are not searched. • ***N***: The number of hours to go back in the Event Log to search for matching events. For example, specify 8 to search the last 8 hours of the Event Log for matching entries. The default is 0.
Event type: Error	Set to **y** to monitor error events. The default is y. If you set the event type to n, an error Event Log entry does not raise an event, is not returned in an event detail message, and is not collected as data if the **Collect data...** parameter is set to y.
Event type: Warning	Set to **y** to monitor warning events. The default is y. If you set the event type to n, a warning Event Log entry does not raise an event, is not returned in an event detail message, and is not collected as data if the **Collect data...** parameter is set to y.
Event type: Information	Set to **y** to monitor information events. The default is y. If you set the event type to n, an informational Event Log entry does not raise an event, is not returned in an event detail message, and is not collected as data if the **Collect data...** parameter is set to y.
Filter: Event ID	Specify a search string that filters the following fields in the Event log: • **Event Category**. Specify one or more text strings to look for in the Category field; separate multiple strings with commas. • **Description**. Specify a detail description or keywords in the description. A string can contain spaces, underscores, and periods; separate multiple entries with commas. For example: `no domain,critical error from the Active Directory`. The search string can contain criteria used to include and exclude entries. The following syntax rules apply: • Separate include and exclude criteria with a colon (:). Strings to the left of the colon are included; strings to the right of the colon are excluded. For example, `zones,caching:primary or secondary`. • Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ`. • If you are specifying only include criteria, the colon is not necessary. For example, `primary DNS domain`. • If you are specifying only exclude criteria, start the search string with a colon. For example, `:online help`.

Description	How to Set It
Filter: Event Description	Specify a search string that filters the following fields in the Event log: • **Event Category**. Specify one or more text strings to look for in the Category field; separate multiple strings with commas. • **Description**. Specify a detail description or keywords in the description. A string can contain spaces, underscores, and periods; separate multiple entries with commas. For example: `no domain,critical error from the Active Directory`. The same search rules as the *Filter: Event ID* parameter apply.
Maximum number of log entries per event message	Set the maximum number of Event Log entries that can be returned in each event report. For example, if this value is set to 30 and 67 Event Log entries are found, three event reports are raised: two reports containing 30 events and one report containing 7 events. The Message column on the **Events** tab in the Operator Console displays the number of events in each event report, the type of log where the events were found, and the event report batch number (the sequential number of the event report). Batch numbers start at 1 for each Knowledge Script iteration. The default is 30 entries per event message.
Event severity when search criteria met	Set the event severity level, from 1 to 40, to indicate the importance of the event when the search criteria is met. The default is 15.
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event when the job fails with an internal error. The default is 5.

ASPNETApplicationRestarted

Use this Knowledge Script to track the number of ASP.NET application restarts during the monitoring interval. AppManager raises an event if the number of ASP.NET applications restarted exceeds the threshold you set.

This Knowledge Script can be set to raise an event when it detects unexpected ASP.NET application restarts.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Note
If the schedule is set to Run Once, the value returned is the current total.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if number of restarts exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for ASP.NET application restarts?	Set to **y** to collect data for reports and graphs. If data is collected, the number of ASP.NET application restarts is returned. The default is n.
Threshold -- Maximum applications restarted	Specify the maximum number of ASP.NET application restarts allowed before AppManager raises an event. The default is 1 restart.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETApplicationRunning

Use this Knowledge Script to monitor the current number of ASP.NET applications running.

This Knowledge Script can be used to track the ASP.NET load on an IIS server. You can set a threshold to determine the number of running applications that raise an event.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Object

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if number of ASP.NET applications running exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for number of ASP.NET applications running?	Set to **y** to collect data for reports and graphs. If data is collected, the current number of ASP.NET applications running is returned. The default is n.
Threshold -- Maximum ASP.NET applications running	Specify the maximum number of running ASP.NET applications allowed before AppManager raises an event. The default is 1 application running.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETErrors

Use this Knowledge Script to monitor the total number of parser, compilation, and runtime errors associated with ASP.NET applications during the monitoring interval.

Use this script to raise an event if errors are occurring. You can set a threshold to determine the number of errors that must occur during the monitoring interval before AppManager raises an event.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Note
If the schedule is set to Run Once, the value returned is the current total.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if number of ASP.NET errors exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for number of ASP.NET errors?	Set to **y** to collect data for reports and graphs. If data is collected, returns the total number of ASP.NET parser, compilation, and runtime errors that occurred during the monitoring interval. The default is n.
Threshold--Maximum ASP.NET errors	Specify the maximum number of ASP.NET errors allowed before AppManager raises an event. The default is 0 errors.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETPipelineInstances

Use this Knowledge Script to monitor the current number of ASP.NET pipeline instances.

This Knowledge Script monitors the overall performance of ASP.NET applications. In most circumstances, it is better for the number of pipeline instances to be low when the server is busy because a low number indicates that the CPU is being used efficiently. Set a threshold to determine the number of pipeline instances that raises an event.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if number of ASP.NET pipeline instances exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for number of ASP.NET pipeline instances?	Set to **y** to collect data for reports and graphs. If data is collected, returns the current number of ASP.NET pipeline instances. The default is n.
Threshold -- Maximum pipeline instances	Specify the maximum number of ASP.NET pipeline instances allowed before AppManager raises an event. The default is 1 pipeline instance.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETReqStat

Use this Knowledge Script to monitor the following:

- Number of current ASP.NET requests
- Number of ASP.NET requests from clients that disconnected during a monitoring interval
- Time taken to execute the most recent ASP.NET request
- ASP.NET requests that are in queue
- ASP.NET request processing rate
- Number of ASP.NET requests that were rejected during a monitoring interval
- Wait time before processing the most recent ASP.NET request

This Knowledge Script consolidates functionality that is also available in seven separate IIS Knowledge Scripts:

- ASPNETRequestCurrent
- ASPNETRequestDisconnected
- ASPNETRequestExecuteTime
- ASPNETRequestQueued
- ASPNETRequestRate:
- ASPNETRequestRejected
- ASPNETRequestWaitTime

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
ASPNETRequestCurrent	Select **Yes** to check for current ASP.NET requests. The default is Yes.
Raise event if number of current ASP.NET requests exceeds threshold?	Select **Yes** to raise an event if the number of ASP.NET requests exceeds the threshold. The default is Yes.

Description	How to Set It
Collect data for number of current ASP.NET requests?	Select **Yes** to collect data for charts and reports. If data is collected, it returns the current number of ASP.NET requests. The default is No.
Threshold -- Maximum current ASP.NET requests	Specify the maximum number of ASP.NET current requests allowed before AppManager raises an event. The default is 1 request.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.
ASPNETRequestDisconnected	Select **Yes** to check for disconnected ASP.NET requests. The default is Yes.
Raise event if number of disconnected ASP.NET requests exceeds threshold?	Select **Yes** to raise an event if the number of disconnected ASP.NET requests exceeds the threshold. The default is Yes.
Collect data for disconnected ASP.NET requests?	Select **Yes** to collect data for charts and reports. If data is collected, it returns the number of ASP.NET requests disconnected because of a communication failure. The default is No.
Threshold -- Maximum disconnected ASP.NET requests	Specify the maximum number of disconnected ASP.NET requests allowed before AppManager raises an event. The default is 0 (no disconnected requests).
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.
ASPNETRequestExecuteTime	Select **Yes** to check the time taken to execute ASP.NET requests. The default is Yes.
Raise event if time required to execute last ASP.NET request exceeds threshold?	Select **Yes** to raise an event if time to execute the last ASP.NET request exceeds the threshold. The default is Yes.
Collect data for time required to execute ASP.NET requests?	Select **Yes** to collect data for charts and reports. If data is collected, it returns the execution time of the last ASP.NET request. The default is No.
Threshold -- Maximum execution time	Specify the maximum ASP.NET request execution time allowed before AppManager raises an event. The default is 100 ms.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.
ASPNETRequestQueued	Select **Yes** to check for queued ASP.NET requests. The default is Yes.
Raise event if number of queued ASP.NET requests exceeds threshold?	Select **Yes** to raise an event if the number of queued ASP.NET request exceeds the threshold. The default is Yes.
Collect data for number of queued ASP.NET requests?	Select **Yes** to collect data for charts and reports. If data is collected, it returns the number of ASP.NET requests currently in all queues. The default is No.
Threshold -- Maximum queued requests	Specify the maximum number of queued requests allowed before AppManager raises an event. The default is 10 requests.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

Description	How to Set It
ASPNETRequestRate	Select **Yes** to check the ASP.NET request processing rate. The default is Yes.
Raise event if number of ASP.NET requests per second exceeds threshold?	Select **Yes** to raise an event if the processing rate for ASP.NET requests fails to meet the threshold. The default is Yes.
Collect data for ASP.NET processing rate?	Select **Yes** to collect data for charts and reports. If data is collected, returns the number of ASP.NET requests processed per second. The default is No.
Threshold -- Minimum processing rate	Specify the minimum processing rate allowed before AppManager raises an event. The default is 10 requests per second.
Threshold -- Minimum requests	Specify the minimum number of ASP.NET requests processed during the interval for the request processing rate to be calculated. No event is raised if the number of requests processed is less than this value. The default is 300 requests.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.
ASPNETRequestRejected	Select **Yes** to check for rejected ASP.NET requests. The default is Yes.
Raise event if number of rejected ASP.NET requests exceeds threshold?	Select **Yes** to raise an event if the number of rejected ASP.NET requests exceeds the threshold. The default is Yes.
Collect data for number of rejected ASP.NET requests?	Select **Yes** to collect data for charts and reports. If data is collected, it returns the number of ASP.NET requests that were rejected because a queue limit was exceeded. The default is No.
Threshold -- Maximum requests rejected	Specify the maximum number of rejected requests allowed before AppManager raises an event. The default is 0 rejected requests.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.
ASPNETRequestWaitTime	Select **Yes** to check the wait time before processing the most recent ASP.NET request. The default is Yes.
Raise event if wait time for the last ASP.NET request exceeds threshold?	Select **Yes** to raise an event if elapsed time in queue for ASP.NET requests exceed the threshold. The default is Yes.
Collect data for ASP.NET request wait time?	Select **Yes** to collect data for charts and reports. If data is collected, it returns the time (in milliseconds) the last ASP.NET request waited in queue before being processed. The default is No.
Threshold -- Maximum ASP.NET request wait time	Specify the maximum wait time of the last ASP.NET request allowed before AppManager raises an event. The default is 1000 ms (1 sec).
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.
Other settings	
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an unexpected error occurred. The default is 35.

ASPNETRequestCurrent

Use this Knowledge Script to monitor the number of requests currently being handled by the ASP.NET Internet Server application programming interface (ISAPI). This script reports the number of requests in the application request queue.

This Knowledge Script can raise an event if ASP.NET is close to rejecting requests because of request volume.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if number of current ASP.NET requests exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for number of current ASP.NET requests?	Set to **y** to collect data for reports and graphs. If data is collected, returns the current number of ASP.NET requests. The default is n.
Threshold -- Maximum current ASP.NET requests	Specify the maximum number of ASP.NET current requests allowed before AppManager raises an event. The default is 900.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETRequestDisconnected

Use this Knowledge Script to monitor the number of ASP.NET requests that have been disconnected because of a communication problem during the monitoring interval.

This script can raise an event if requests are being disconnected because of communication problems.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if number of disconnected ASP.NET requests exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for disconnected ASP.NET requests?	Set to **y** to collect data for reports and graphs. If data is collected, returns the number of ASP.NET requests disconnected because of a communication failure. The default is n.
Threshold -- Maximum disconnected ASP.NET requests	Specify the maximum number of disconnected ASP.NET requests allowed before AppManager raises an event. The default is 0 (no disconnected requests).
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETRequestExecuteTime

Use this Knowledge Script to monitor the time required to execute the last ASP.NET request.

This script raises an event if requests are taking an unexpectedly long time to execute.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if time required to execute last ASP.NET request exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for time required to execute request?	Set to **y** to collect data for reports and graphs. If data is collected, returns the execution time of the last ASP.NET request. The default is n.
Threshold -- Maximum execution time	Specify the maximum ASP.NET request execution time allowed before AppManager raises an event. The default is 100 ms.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETRequestQueued

Use this Knowledge Script to monitor the number of ASP.NET requests currently in all queues.

Note
There is a queue between inetinfo and aspnet_wp, and there is a queue for each virtual directory.

This script raises an event if too many requests are being queued.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if number of queued ASP.NET requests exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for number of queued ASP.NET requests?	Set to **y** to collect data for reports and graphs. If data is collected, returns the number of ASP.NET requests currently in all queues. The default is n.
Threshold -- Maximum queued requests	Specify the maximum number of queued requests allowed before AppManager raises an event. The default is 10 requests.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETRequestRate

Use this Knowledge Script to monitor the number of ASP.NET requests processed per second. Two thresholds can be set. The request rate is not calculated unless a minimum number of ASP.NET requests are processed during the monitoring interval. The request rate is then calculated and compared with the minimum number of ASP.NET requests processed per second threshold. If the request rate falls below the minimum, AppManager raises an event.

Use this script to monitor the overall performance of ASP.NET applications.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if processing rate for ASP.NET requests fails to meet threshold?	Set to **y** to raise events. The default is y.
Collect data for processing rate?	Set to **y** to collect data for reports and graphs. If data is collected, returns the number of ASP.NET requests processed per second. The default is n.
Threshold -- Minimum processing rate	Specify the minimum processing rate allowed before AppManager raises an event. The default is 10 requests per second.
Threshold -- Minimum requests	Specify the minimum number of ASP.NET requests processed during the interval for the request processing rate to be calculated. No event is raised if the number of requests processed is less than this value. The default is 300 requests.
Event severity when processing rate threshold not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETRequestRejected

Use this Knowledge Script to monitor the number of ASP.NET requests that were rejected during the monitoring interval.

This script raises an event if the number of rejected ASP.NET requests exceeds the threshold you set, indicating that insufficient server resources were available to process them.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if number of rejected ASP.NET requests exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for number of rejected ASP.NET requests?	Set to **y** to collect data for reports and graphs. If data is collected, the number of ASP.NET requests that were rejected because a queue limit was exceeded is returned. The default is n.
Threshold -- Maximum requests rejected	Specify the maximum number of rejected requests allowed before AppManager raises an event. The default is 0 rejected requests.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETRequestWaitTime

Use this Knowledge Script to monitor the time in milliseconds that the last ASP.NET request waited in a queue before being processed.

This script raises an event if the length of time that requests are in queue exceeds the threshold you set.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if elapsed time in queue exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for ASP.NET request wait time?	Set to **y** to collect data for reports and graphs. If data is collected, the time (in milliseconds) the last ASP.NET request waited in queue before being processed is returned. The default is n.
Threshold -- Maximum ASP.NET request wait time	Specify the maximum wait time of the last ASP.NET request allowed before AppManager raises an event. The default is 1000 ms (1 sec).
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETWorkerProcessCPU

Use this Knowledge Script to monitor the CPU utilization of the ASP.NET worker processes: `w3wp` or `aspnet_wp`.

This script raises an event if the percentage of CPU time being used by the ASP.NET worker processes exceeds the threshold you set.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if ASP.NET worker process CPU utilization exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for ASP.NET worker process CPU utilization?	Set to **y** to collect data for reports and graphs. The default is n. If data is collected, the percentage of CPU time used by the ASP.NET worker processes is returned.
Threshold -- ASP.NET worker process CPU utilization	Specify the maximum CPU percentage used by the ASP.NET worker processes that is allowed before AppManager raises an event. The default is 70%.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETWorkerProcessExcepRate

Use this Knowledge Script to monitor the current exception rate for the common language runtime (CLR) in ASP.NET worker processes: `w3wp` or `aspnet_wp`.

AppManager raises an event if CLR exceptions are thrown in ASP.NET worker processes at an unexpectedly high rate.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event when rate of ASP.NET CLR exceptions exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for ASP.NET CLR exceptions rate?	Set to **y** to collect data for reports and graphs. The default is n. If data is collected, the number of CLR exceptions thrown per second by ASP.NET worker processes is returned.
Threshold -- Maximum ASP.NET CLR exception rate	Specify the maximum number of CLR exceptions thrown per second by ASP.NET worker processes that is allowed before AppManager raises an event. The default is 0.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETWorkerProcessExceptions

Use this Knowledge Script to monitor the current total number of exceptions thrown by the common language runtime (CLR) in ASP.NET worker processes: `w3wp` or `aspnet_wp`.

This script raises an event if an unusually large number of CLR exceptions are thrown in ASP.NET worker processes.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event when number of ASP.NET CLR exceptions exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for ASP.NET CLR exceptions?	Set to **y** to collect data for reports and graphs.The default is n. If data is collected, returns the current total number of CLR exceptions thrown by ASP.NET worker processes.
Threshold -- Maximum ASP.NET CLR exceptions	Specify the maximum number of CLR exceptions thrown by ASP.NET worker processes that is allowed before AppManager raises an event. The default is 0.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETWorkerProcessMemory

Use this Knowledge Script to monitor the nonshared, or "private," memory usage of the ASP.NET worker processes: `w3wp` or `aspnet_wp`.

This script raises an event if ASP.NET worker processes use an unusually large amount of nonshared memory.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if private memory utilization exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for total private memory utilization?	Set to **y** to collect data for reports and graphs. If data is collected, returns the number of bytes of private memory used by both ASP.NET worker processes during the monitoring interval. The default is n.
Threshold -- Maximum private memory utilized	Specify the maximum number of bytes of private memory used by the ASP.NET worker processes that is allowed before AppManager raises an event. The default is 25,000 KB.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETWorkerProcessRestarted

Use this Knowledge Script to monitor the number of times an ASP.NET worker process, `w3wp` or `aspnet_wp`, was restarted during the monitoring interval

This script raises an event if worker processes are unexpectedly restarting.

Versions of IIS Supported

6.0 and later, with the .NET Framework installed.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if number of times ASP.NET worker processes were restarted exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for number of ASP.NET worker process restarts?	Set to **y** to collect data for reports and graphs. If data is collected, returns the number of ASP.NET worker process restarts. The default is n.
Threshold -- Maximum ASP.NET worker process restarts	Specify the maximum number of ASP.NET worker processes that can be restarted during the monitoring interval before AppManager raises an event. The default is 1.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPNETWorkerProcessRunning

Use this Knowledge Script to monitor the number of running ASP.NET worker process: `aspnet_wp`.

This script raises an event if more ASP.NET worker processes are running than expected.

Versions of IIS Supported

6.0 and later

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Raise event if number of running ASP.NET worker processes exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for currently running ASP.NET worker processes?	Set to **y** to collect data for reports and graphs. If data is collected, the number of ASP.NET worker processes running during the monitoring interval is returned. The default is n.
Threshold -- Maximum number of ASP.NET worker processes currently running	Specify the maximum number of ASP.NET worker processes that can be running before AppManager raises an event. The default is 2.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPQueueBusy

Use this Knowledge Script to monitor the number of ASP requests currently in the queue. If the number of queued requests exceeds the threshold for a specified number of monitoring intervals, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of ASP queued requests exceeds threshold for *N* consecutive intervals?	Set to **y** to raise events. The default is y.
Collect data for ASP queued requests?	Set to **y** to collect data for charts and reports. If set to y, this script returns the number of ASP requests in the queue. The default is n.
Threshold -- Maximum ASP queue length	Specify the maximum number of ASP requests allowed in the queue before AppManager raises an event. The default is 3 requests.
Threshold -- Maximum number of consecutive intervals where queue length exceeds threshold	Specify the maximum number of consecutive intervals the queue length can exceed the threshold before AppManager raises an event. The default is 3 intervals.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPRegistryChange

Use this Knowledge Script to monitor changes to Windows Registry parameters. Valid keys include HKEY_LOCAL_MACHINE, HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, and HKEY_USERS. If a registry key or value is added, changed, or deleted, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if changes to registry keys detected?	Set to **y** to raise events. The default is y.
Collect data for changes to registry keys?	Set to **y** to collect data for charts and reports. If set to y, returns the number of changes to the Windows Registry since the previous job ran. The default is n.
Root registry key to monitor	Specify the root registry key to monitor. Valid root options are: • HKEY_LOCAL_MACHINE • HKEY_CLASSES_ROOT • HKEY_CURRENT_USER • HKEY_USERS The default is HKEY_LOCAL_MACHINE.
Pathname	Specify the full path to the registry key. The default path is SYSTEM\CurrentControlSet\Services\W3SVC.
Sub-level	Specify the number of descending key levels below the path name to monitor. The default is 2 levels deep.
Sub-keys to exclude (separated by commas)	Specify any sub-keys to exclude from monitoring. Separate sub-keys using commas; do not add spaces between sub-key entries. For example, to exclude "Beep" and "Afd" under the CurrentControlSet sub-key, specify the following: SYSTEM\CurrentControlSet\Services\Beep,SYSTEM\CurrentControlSet\Services\Afd
Event severity when change detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the changed is detected. The default is 8.
Event severity for errors accessing the registry	Set the event severity level, from 1 and 40, to indicate the importance of the event. The default is 35.

ASPReqStat

Use this Knowledge Script to monitor the number of ASP request errors per second, different types of ASP request failures during an interval, and ASP sessions that timed out during an interval.

This Knowledge Script consolidates the functionality that is also available in three separate IIS Knowledge Scripts:

- ASPRequestError
- ASPRequestFailed
- ASPSessionTimeout

Versions of IIS Supported

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
ASPRequestError	Select **Yes** to check for ASP request errors. The default is Yes.
Raise an event if ASP request error rate exceeds threshold?	Select **Yes** to raise an event if the ASP request error rate exceeds the threshold. The default is Yes.
Collect data for current ASP request errors?	Select **Yes** to collect data for charts and reports. The default is No.
Threshold -- Maximum current ASP request error rate	Specify the maximum number of errors per second allowed before AppManager raises an event. The default is 1 error per second.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 5.
ASPRequestFailed	Select **Yes** to check for ASP request failures. The default is Yes.
Raise event if number of errors exceeds any threshold?	Select **Yes** to raise an event if the number of errors exceeds any threshold. The default is Yes.
Collect data for number of ASP request failures?	Select **Yes** to collect data for charts and reports. If enabled, this script returns the number of failure, rejection, and timeout errors during an interval. The default is No.
Threshold -- Maximum number of failure errors	Specify the maximum number of failure errors allowed before AppManager raises an event. The default is 25 errors.
Threshold -- Maximum number of rejected errors	Specify the maximum number of rejection errors allowed before AppManager raises an event. The default is 25 errors.

Description	How to Set It
Threshold -- Maximum number of timeout errors	Specify the maximum number of timeout errors allowed before AppManager raises an event. The default is 25 errors.
Event severity when any threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 5.
ASPRequestTimeout	Select **Yes** to check for ASP sessions that timed out during a monitoring interval. The default is Yes.
Raise event if number of timed-out ASP sessions exceeds threshold?	Select **Yes** to raise an event if the number of ASP sessions exceeds the threshold. The default is Yes.
Collect data for number of timed-out ASP sessions?	Select **Yes** to collect data for charts and reports. If selected, this script returns the number of sessions that timed out during a monitoring interval. The default is No.
Threshold -- Maximum number of timed-out sessions	Specify the maximum number of sessions that can time out during an interval before AppManager raises an event. The default is 25 sessions.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Other settings	
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.

ASPRequestError

Use this Knowledge Script to monitor the number of ASP request errors per second. Errors that can occur in response to an ASP request include connection errors, compile errors, and runtime errors. If the number of errors per second exceeds the threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if ASP request error rate exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for current ASP request errors?	Set to **y** to collect data for charts and reports. If set to y, this script returns the current number of ASP request errors per second. The default is n.
Threshold -- Maximum current ASP request error rate	Specify the maximum number of errors per second allowed before AppManager raises an event. The default is 1 error per second.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.

ASPRequestFailed

Use this Knowledge Script to monitor the number of ASP request failures during the monitoring interval, by error type. ASP requests can fail for the following reasons:

- Failures
- Rejection because of insufficient resources available to queue the request
- Timeout before the request can be completed

If the number of failure errors, rejected errors, or timeout errors exceeds the thresholds you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 30 minutes**.

Note
If the schedule is set to Run Once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of errors exceeds any threshold?	Set to **y** to raise events if any of the thresholds is exceeded. The default is y.
Collect data for number of ASP request errors?	Set to **y** to collect data for charts and reports. If set to y, returns the number of failure, rejection, and timeout errors during an interval. The default is n.
Threshold -- Maximum number of failure errors	Specify the maximum number of failure errors allowed before AppManager raises an event. The default is 25 errors.
Threshold -- Maximum number of rejected errors	Specify the maximum number of rejection errors allowed before AppManager raises an event. The default is 25 errors.
Threshold -- Maximum number of timeout errors	Specify the maximum number of timeout errors allowed before AppManager raises an event. The default is 25 errors.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

ASPSessionTimeout

Use this Knowledge Script to monitor the number of ASP sessions that timed out during a monitoring interval. If the number of ASP sessions that timed out exceeds the threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 5 minutes**.

Note
If the schedule is set to Run Once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of timed-out ASP sessions exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for number of timed-out ASP sessions?	Set to **y** to collect data for charts and reports. If set to y, this script returns the number of sessions that timed out during a monitoring interval. The default is n.
Threshold -- Maximum number of timed-out sessions	Specify the maximum number of sessions that can time out during an interval before AppManager raises an event. The default is 25 sessions.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

ASPThroughput

Use this Knowledge Script to monitor the current number of ASP requests processed per second. If the current ASP request rate exceeds the threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of ASP requests processed per second exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for average number of ASP requests processed per second?	Set to **y** to collect data for charts and reports. If set to y, returns the average number of ASP requests processed per second. The default is n.
Threshold -- Maximum number of ASP requests processed per second	Specify the maximum number of ASP requests per second allowed before AppManager raises an event. The default is 100 requests per second.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

CacheHitRatio

Use this Knowledge Script to monitor the cache hit ratio for cache requests: the total number of cache hits and misses, and the cache hit ratio.

The cache hit ratio is the percentage of time information is found in the cache. A low cache hit ratio might indicate that the information most commonly requested is not stored in the cache and that the contents of the cache need to be reexamined. If the cache hit ratio falls below the minimum threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

IIS servers

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if cache hit ratio fails to meet threshold?	Set to **y** to raise events. The default is y.
Collect data for cache hits, cache misses, and cache hit ratio?	Set to **y** to collect data for charts and reports. If set to y, the script returns the cache hit ratio. The default is n.
Threshold -- Minimum cache hit ratio	Specify the minimum number of cache hits required during any interval before AppManager raises an event. The default is 50%.
Event severity when threshold not met	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

CentralizedBinaryLogging

Use this Knowledge Script to scan the IIS centralized binary logging file for information by choosing from a list of filter criteria.

IIS used two types of logging:

- Normal: Creates one log file per Web site. Depending on the number of Web sites, the corresponding folders (`w3svc*`) are created under the log file directory at `C:\WINDOWS\system32\LogFiles`.
- Binary: Creates one folder under the log files directory at `C:\WINDOWS\system32\LogFiles\W3SVC`.

Usually an IIS server hosts many Web sites. In such a situation, creating many log files and writing all the log data to a disk consumes CPU and memory resources. This creates performance and scalability issues. Centralized binary logging is a process where multiple Web sites send binary, unformatted log data to a single log file. Centralized binary logging minimizes the amount of system resources used for logging, while providing detailed log data, which is useful in troubleshooting applications.

This Knowledge Script converts the binary file into text format. The corresponding folders are created according to the Web site information in the binary file. These folders do not interfere with the functioning of the log files. Manually deleting the folders does not have any effect on the functioning of the binary log.

If log entries matching the filter criteria are found, AppManager raises an event.

Note
File Transfer Protocol (FTP), Network News Transfer Protocol (NNTP), and Simple Mail Transfer Protocol (SMTP) do not support Centralized Binary Logging.

Prerequisite

To enable the Knowledge Script to read the binary logging file, install Microsoft Log Parser.

For more information, see http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&displaylang=en.

Version Compatibility

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default schedule of this script is **Once daily**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if log entries match search criteria?	Select **Yes** to raise an event if log entries match search criteria. The default is Yes
Collect data for matching log entries?	Select **Yes** to collect data for matching log entries for charts and graphs. The default is No.
Filter: Bytes received greater than	Specify the number of bytes received that you want to search for in the centralized binary logging file. Numbers in this field are “greater than” values. For example, if you specify `200`, this script searches the Bytes Received column for values greater than 200. The default is 200 bytes received.
Filter: Bytes sent greater than	Specify the number of bytes sent that you want to search for in the centralized binary logging file. Numbers in this field are “greater than” values. For example, if you specify `200`, this script searches the Bytes Sent column for values greater than 200. The default is 200 bytes sent.
Filter: Client IP	Specify the Web address or IP address to search for in the IIS Web site log.
Filter: Operation type	Specify the operation type to search for. For example, type `get` or `post`. Specify one type.
Filter: Protocol status	Specify the HTTP protocol status code to search for. For example, `200`.
Filter: Protocol version	Specify the protocol version number to search for. For example, HTTP 1.0.
Filter: URI Stem	Specify the Uniform Resource Identifier (URI) Stem of the server to search for. URI is the addressing technology for identifying resources on the Internet or private Intranet.
Filter: Server IP	Specify the IP address of the server to search for.
Filter: Server name	Specify the name of the server to search for.
Filter: Time taken greater than	Specify the length of time an HTTP action (for example, `get` or `post`) takes to complete. Numbers in this field are “greater than” values. For example, if you type `200`, this script searches the Time Taken column for values greater than 200. The default is 200 milliseconds (ms).
Filter: Windows status	Specify the Windows status code to search for. For example, `200`.
Event severity when search criteria met	Set the event severity level, from 1 to 40, to indicate the importance of the event. Adjust the severity depending on which types of events you check for. The default is 8.

CGIRequests

Use this Knowledge Script to monitor the CGI requests for a Web site. A CGI (Common Gateway Interface) request serves as an interface between an HTTP request and the execution of a program on the Web server. If the number of CGI requests exceeds the threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

Discovered Web sites

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if current number of CGI requests exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for current number of CGI requests?	Set to **y** to collect data for charts and reports. If set to y, returns the number of CGI requests completed. The default is n.
Threshold -- Maximum number of CGI requests	Specify the maximum number of CGI requests that are allowed before AppManager raises an event. The default is 200 requests.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

CpuHigh

Use this Knowledge Script to monitor the CPU utilization of IIS application processes. If the amount of CPU time used by any IIS process exceeds the threshold you set, AppManager raises an event.

You can select which processes to monitor. The processes to monitor depend on the version of IIS you are running.

IIS 6.0:

- When running in IIS 5.0 compatibility mode, `inetinfo.exe`, for in-process applications, or `dllhost.exe`, for out-of-process applications. One `dllhost.exe` process is for the pooled applications, and one is for each isolated out-of-process application. If you have the .NET Framework installed on IIS 6.0, you can also monitor `aspnet_wp` for any ASP.NET applications.
- When running in worker process isolation mode, `w3wp.exe` for multiple processes.

IIS 7.0 and IIS 7.5:

- `inetinfo` with IIS 6.0 compatibility option enabled
- `w3wp`

Versions of IIS Supported

6.0 and later.

Resource Objects

IIS servers

Default Schedule

The default interval is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if CPU utilization of any process exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for CPU utilization by process?	Set to **y** to collect data for charts and reports. If set to y, this script returns the CPU utilization of the named application process. The default is n.
Process names to monitor (separated by commas)	Specify the names of the application processes to monitor. Separate multiple entries with commas. For example: `inetinfo,dllhost`.
Threshold -- Maximum CPU utilization for any process	Specify the maximum percentage of CPU resources the selected processes can use before AppManager raises an event. The default is 60%.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

FTPBytes

Use this Knowledge Script to monitor the total number of bytes transferred per second to and from an FTP site. If the byte transfer rate exceeds the threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

FTP sites

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of bytes transferred per second exceeds a threshold?	Set to **y** to raise events. The default is n.
Collect data for current transfer rate (bytes sent, bytes received)?	Set to **y** to collect data for charts and reports. If set to y, returns the number of bytes transferred per second. The default is n.
Threshold -- Maximum bytes received per second	Specify the maximum bytes per second that can be received by the FTP site before AppManager raises an event. The default is 64000 bytes per second.
Threshold -- Maximum bytes sent per second	Specify the maximum bytes per second that can be sent by the FTP site before AppManager raises an event. The default is 64000 bytes per second.
Event severity when either threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

FTPConnections

Use this Knowledge Script to monitor the current number of connections from anonymous and non-anonymous (user) accounts to an FTP site. If the number of FTP site connections exceeds the threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

FTP sites

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if current number of connections exceeds either threshold?	Set to **y** to raise events. The default is n.
Collect data for current FTP connections (from anonymous or non-anonymous accounts)?	Set to **y** to collect data for charts and reports. If set to y, this script returns the number of connections from anonymous and user accounts to the FTP site. By default, data is collected.
Threshold -- Maximum connections from anonymous accounts	Specify the maximum number of connections allowed from anonymous accounts to the FTP site before AppManager raises an event. The default is 64 connections.
Threshold -- Maximum connections from non-anonymous (user) accounts	Specify the maximum number of connections allowed from non-anonymous (user) accounts to the FTP site before AppManager raises an event. The default is 64 connections.
Event severity when either threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 12.

FTPConnectionsInterval

Use this Knowledge Script to monitor the number of connections to an FTP site, and totals for all monitored sites, from anonymous and user accounts during the monitoring interval. If the number of FTP connections exceeds the threshold, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

FTP sites

Default Schedule

The default interval for this script is **Every 30 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of connections exceeds any threshold?	Set to **y** to raise events. The default is y.
Collect data for number of connections per site, and total for all sites?	Set to **y** to collect data for charts and reports. If set to y, returns the number of FTP connections during the monitoring interval. The default is n.
Threshold -- Maximum connections to FTP site from anonymous accounts	Specify the maximum number of FTP site connections that can come from anonymous accounts before AppManager raises an event. The default is 64 connections.
Threshold -- Maximum connections to FTP site from non-anonymous accounts	Specify the maximum number of FTP site connections that can come from non-anonymous (user) accounts before AppManager raises an event. The default is 64 connections.
Threshold -- Maximum total connections to all FTP sites from anonymous accounts	Specify the maximum total number of connections to all FTP sites that can come from anonymous accounts before AppManager raises an event. The default is 64 connections.
Threshold -- Maximum total connections to all FTP sites from non-anonymous accounts	Specify the maximum total number of connections to all FTP sites that can come from non-anonymous (user) accounts before AppManager raises an event. The default is 64 connections.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 12.

FTPConnectionUtil

Use this Knowledge Script to monitor the percentage of connections to an FTP site that are being utilized. If the percentage of FTP connections exceeds the threshold you set, AppManager raises an event.

If you receive an event stating that the "maximum number of connections" value cannot be retrieved, specify the maximum number of connections allowed on the FTP site on which you are running the Knowledge Script for the **Maximum connections allowed** parameter. Information about the maximum number of connections allowed on an FTP server can be found in the IIS Manager.

If your FTP connections are unlimited, either use the default value or refer to the IIS documentation for information about how to calculate the total number available connections.

No data point is collected for utilization percentage when the Maximum Connections, taken either from IIS itself or from the **Maximum connections allowed** parameter, is 0.

Versions of IIS Supported

6.0 and later.

Resource Objects

FTP sites

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if connection utilization exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for current connections and connection utilization?	Set to **y** to collect data for charts and reports. If set to y, returns the number of FTP connections and connection utilization (%). No data point is collected for the percentage of utilization when the Maximum Connections is 0. The default is n.
Threshold -- Maximum connection utilization	Specify the maximum percentage of available FTP connections that can be used before AppManager raises an event. The default is 90%.
Maximum connections allowed on this site	If the "maximum number of connections" value cannot be retrieved from the site, specify the maximum number of connections allowed on the FTP site where this script is being run. The default is 5000 FTP connections.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 12.

FTPFiles

Use this Knowledge Script to monitor the total number of files sent to and received from an FTP site during the monitoring interval. If the number of transferred files exceeds the threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and higher.

Resource Objects

FTP sites

Default Schedule

The default interval is **Every 30 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of files sent or received exceeds threshold?	Set to **y** to raise events. The default is n.
Collect data for files sent or files received?	Set to **y** to collect data for charts and reports. If set to y, returns the number of files being sent and received by the FTP site during an interval. By default, data is collected.
Threshold -- Maximum files received	Specify the maximum number of files that can be received by the FTP site during an interval before AppManager raises an event. The default is 640 files.
Threshold -- Maximum files sent	Specify the maximum number of files that can be sent by the FTP site during an interval before AppManager raises an event. The default is 640 files.
Event severity when either threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

FTPStatistics

Use this Knowledge Script to monitor the current number of connections to FTP sites, number of FTP site connections, and percentage of FTP connections being utilized.

This Knowledge Script consolidates functionality that is also available in three separate IIS Knowledge Scripts:

- FTPConnections
- FTPConnectionsInterval
- FTPConnectionUtil

If you receive an event stating that the "maximum number of connections" value cannot be retrieved, specify the maximum number of connections allowed on the FTP site on which you are running the Knowledge Script for the **Maximum connections allowed on this site** parameter. Information about the maximum number of connections allowed on an FTP server can be found in the IIS Manager.

If your FTP connections are unlimited, either use the default value or refer to the IIS documentation for information on calculating the total number available connections.

No data point is collected for utilization percentage when the Maximum Connections, taken either from IIS itself or from the **Maximum connections allowed on this site** parameter, is 0.

Versions of IIS Supported

6.0 and later.

Resource Objects

FTP sites

Default Schedule

The default interval is **Every 30 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
FTPConnections	Select **Yes** to check for the current number of connections to FTP sites. The default is Yes.
Raise event if current number of connections exceeds either threshold?	Select **Yes** to raise events. The default is Yes.
Collect data for current FTP connections (from anonymous or non-anonymous accounts)?	Select **Yes** to collect data for charts and reports. If set to Yes, this script returns the number of connections from anonymous and user accounts to the FTP site. The default is No.

Description	How to Set It
Threshold -- Maximum connections from anonymous accounts	Specify the maximum number of connections allowed from anonymous accounts to the FTP site before AppManager raises an event. The default is 64 connections.
Threshold -- Maximum connections from non-anonymous (user) accounts	Specify the maximum number of connections allowed from non-anonymous (user) accounts to the FTP site before AppManager raises an event. The default is 64 connections.
Event severity when either threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 12.
FTPConnectionsInterval	Select **Yes** to check for the number of connections to FTP sites. The default is Yes.
Raise event if number of connections exceeds either threshold?	Select **Yes** to raise events. The default is Yes.
Collect data for number of connections per site and total for all sites?	Select **Yes** to collect data for charts and reports. If set to Yes, returns the number of FTP connections during the monitoring interval. The default is No.
Threshold -- Maximum connections to FTP site from anonymous accounts	Specify the maximum number of FTP site connections from anonymous accounts before AppManager raises an event. The default is 64 connections.
Threshold -- Maximum connections to FTP site from non-anonymous (user) accounts	Specify the maximum number of FTP site connections from non-anonymous accounts before AppManager raises an event. The default is 64 connections.
Threshold -- Maximum total connections to all FTP sites from anonymous accounts	Specify the maximum total number of connections to all FTP sites from anonymous accounts before AppManager raises an event. The default is 64 connections.
Threshold -- Maximum total connections to all FTP sites from non-anonymous (user) accounts	Specify the maximum total number of connections to all FTP sites from non-anonymous accounts before AppManager raises an event. The default is 64 connections.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 12.
FTPConnectionUtil	Select **Yes** to check for the percentage of connections to an FTP site that are being utilized. The default is No.
Raise event if connection utilization exceeds threshold?	Select **Yes** to raise events. The default is Yes.
Collect data for current connections and connection utilization?	Select **Yes** to collect data for charts and reports. If set to Yes, returns the number of FTP connections and connection utilization (%). No data point is collected for the percentage of utilization when the **Maximum Connections** is 0. The default is No.
Threshold -- Maximum connection utilization	Specify the maximum percentage of available FTP connections before AppManager raises an event. The default is 90%.
Maximum connections allowed on this site	If the “maximum number of connections” value cannot be retrieved from the site, specify the maximum number of connections allowed on the FTP site where this script is being run. The default is 5000 FTP connections.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 12.
Other settings	
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.

FTPTransStat

Use this Knowledge Script to monitor the rate of bytes transferred per second and the total number of files sent to and received from the FTP server.

This Knowledge Script consolidates functionality that is also available in two separate IIS Knowledge Scripts:

- FTPBytes
- FTPFiles

Versions of IIS Supported

6.0 and later.

Resource Objects

FTP sites

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
FTPBytes	Select **Yes** to check the total number of bytes transferred per second to and from an FTP site. The default is Yes.
Raise event if number of bytes transferred per second exceeds threshold?	Select **Yes** to raise events. The default is Yes.
Collect data for current transfer rate (bytes sent, bytes received)?	Select **Yes** to collect data for charts and reports. If set to Yes, returns the number of bytes transferred per second. The default is No.
Threshold -- Maximum bytes received per second	Specify the maximum bytes per second that can be received by the FTP site before AppManager raises an event. The default is 64000 bytes per second.
Threshold -- Maximum bytes sent per second	Specify the maximum bytes per second that can be sent by the FTP site before AppManager raises an event. The default is 64000 bytes per second.
Event severity when either threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
FTPFiles	Select **Yes** to check the total number of files sent to and received from an FTP site during the monitoring interval. The default is Yes.
Raise event if number of files sent or received exceeds threshold?	Select **Yes** to raise events. The default is Yes.
Collect data for files sent or files received?	Select **Yes** to collect data for charts and reports. If set to Yes, returns the number of files sent and received by the FTP site during an interval. The default is No.

Description	How to Set It
Threshold -- Maximum files received	Specify the maximum number of files that can be received by the FTP site during an interval before AppManager raises an event. The default is 640 files.
Threshold -- Maximum files sent	Specify the maximum number of files that are sent by the FTP site during an interval before AppManager raises an event. The default is 640 files.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Other settings	
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.

HealthCheck

Use this Knowledge Script to check the status of IIS services and Web sites. If any IIS service, such as `W3svc`, or Web site is not running, AppManager raises an event. Optionally, the IIS service or Web site can automatically be re-started.

Versions of IIS Supported

6.0 and later.

Resource Objects

IIS services and Web sites

Default Schedule

The default interval is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Auto-start service or Web site?	Set to **y** to automatically restart down services or Web sites. The default value is **y**.
Event severity: Auto-start...	Set the event severity level, from 1 to 40, to indicate the importance when auto-start: • **... fails**. Specify a value that indicates the service or site is down and AppManager for IIS cannot restart it. The default is 5. • **... succeeds**. Specify a value that indicates the service or site was down and AppManager for IIS successfully restarted it. The default is 25. • **...Site or service is down and auto-start not enabled**. Specify a value to indicate the service or site is down and AppManager for IIS has been set not to restart. The default is 18.
Collect data for site or service status?	Set to **y** to collect data for charts and reports. The default is n.

HTTPBytes

Use this Knowledge Script to monitor the total number of bytes transferred per second to and from a Web site. If the total number of transferred bytes exceeds the thresholds you set, AppManager raises an event.

This script supports "dynamic observation" of Web sites. Dynamically observed Web sites are new sites that AppManager for IIS has observed while monitoring your IIS servers. These sites are included in jobs, but they cannot be monitored until you discover them by running the Discovery_IIS Knowledge Script again.

If you select a subset of Web sites for the job but leave the **Dynamically observe sites at each interval?** parameter enabled, this script will still do dynamic observation, and results will be returned for all Web sites, not just the subset selected. To limit results, disable the **Dynamically observe...** parameter.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web sites

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe Web sites at each interval?	Set to **y** to dynamically observe new Web sites at each monitoring interval. The default is y.
Exclude Web sites (separate names with commas)	Specify the name of any site you want to exclude. You can exclude multiple sites, separated by commas with no spaces. For example: `site1,site2`. **Note** If you are not dynamically observing sites, this parameter is ignored.
Raise event if number of bytes transferred per second exceeds a threshold?	Set to **y** to raise events. The default is y.
Collect data for current transfer rate (bytes sent, bytes received)?	Set to **y** to collect data for charts and reports. If set to y, returns the byte transfer rate for the HTTP server. By default, data is collected.
Threshold -- Maximum bytes received per second	Specify the maximum bytes per second that can be received by the HTTP server before AppManager raises an event. The default is 64000 bytes per second.
Threshold -- Maximum bytes sent per second	Specify the maximum bytes per second that can be sent by the HTTP server before AppManager raises an event. The default is 64000 bytes per second.
Event severity when either threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.

HTTPBytesInterval

Use this Knowledge Script to monitor the number of bytes transferred to and from Web sites, and totals for all monitored sites, during the monitoring interval. If the number of transferred bytes exceeds any of the thresholds you set, AppManager raises an event.

This script supports "dynamic observation" of Web sites. Dynamically observed Web sites are new sites that AppManager for IIS has observed while monitoring your IIS servers. These sites are included in jobs, but they cannot be monitored until you discover them by running the Discovery_IIS Knowledge Script again.

If you select a subset of Web sites for the job but leave the **Dynamically observe sites at each interval?** parameter set to y, this script will still do dynamic observation, and results will be returned for all Web sites, not just the subset selected. To limit results, set the **Dynamically observe...** parameter to n. You can disable monitoring of totals for all sites by typing "_Total" for the **Exclude Web sites** parameter.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web sites

Default Schedule

The default interval is **Every 30 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe Web sites at each interval?	Set to **y** to dynamically observe new Web sites at each monitoring interval. The default is y.
Exclude Web sites	Specify the name of any site you want to exclude. You can exclude multiple sites, separated by commas with no spaces. For example: `site1,site2`. Specify "_Total" to disable monitoring of totals. **Note** If you are not dynamically observing sites, this parameter is ignored.
Raise event if number of bytes transferred exceeds any threshold?	Set to **y** to raise events. The default is y.
Collect data for transfer rate (bytes sent, bytes received)?	Set to **y** to collect data for charts and reports. If set to y, returns the number of bytes transferred to and from the HTTP server during the monitoring interval. The default is n.
Threshold -- Maximum bytes received by Web site	Specify the maximum number of bytes that can be received by a Web site during a monitoring interval before AppManager raises an event. The default is 64000 bytes.

Description	How to Set It
Threshold -- Maximum bytes sent by Web site	Specify the maximum number of bytes that can be sent by a Web site during a monitoring interval before AppManager raises an event. The default is 64000 bytes.
Threshold -- Maximum total bytes received by all Web sites	Specify the maximum number of bytes that can be received by all monitored Web sites during a monitoring interval before AppManager raises an event. The default is 64000 bytes.
Threshold -- Maximum total bytes sent by all Web sites	Specify the maximum total number of bytes that can be sent by all monitored Web sites during a monitoring interval before AppManager raises an event. The default is 64000 bytes.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.

HTTPConnectionsInterval

Use this Knowledge Script to monitor the number of Web site connections, and totals for all Web sites, from anonymous and non-anonymous (or user) accounts during the monitoring interval. This Knowledge Script monitors the number of connections established after the previous iteration. If the number of Web site connections exceeds any threshold, AppManager raises an event.

This script supports "dynamic observation" of Web sites. Dynamically observed Web sites are new sites that AppManager for IIS has observed while monitoring your IIS servers. These sites are included in jobs, but they cannot be monitored until you discover them by running the Discovery_IIS Knowledge Script again.

If you select a subset of Web sites for the job but leave the **Dynamically observe sites at each interval?** parameter set to y, this script will still do dynamic observation, and results will be returned for all Web sites, not just the subset selected. To limit results, set the **Dynamically observe...** parameter to n. You can disable monitoring of totals for all sites by typing "_Total" for the **Exclude Web sites** parameter.

Versions of IIS Supported

6.0 and later.

Resource Objects

Discovered Web sites

Default Schedule

The default interval for this script is **Every 30 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe Web sites at each interval?	Set to **y** to dynamically observe new Web sites at each monitoring interval. The default is y.
Exclude Web sites (separate names with commas)	Specify the name of any request you want to exclude. You can exclude multiple sites, separated by commas with no spaces. For example: `site1,site2`. Specify "_Total" to disable monitoring of totals for all sites. **Note** If you are not dynamically observing sites, this parameter is ignored.
Raise event if number of connections exceeds a threshold?	Set to **y** to raise events. The default is y.
Collect data for number of connections?	Set to **y** to collect data for charts and reports. If set to y, returns the number of Web server connections during the monitoring interval. The default is n.

Description	How to Set It
Threshold -- Maximum connections to Web site from anonymous accounts	Specify the maximum number of Web site connections from anonymous accounts that can be open during the monitoring interval. The default is 64
Threshold -- Maximum connections to Web site from non-anonymous (user) accounts	Specify the maximum number of Web site connections from non-anonymous (user) accounts that can be open during the monitoring interval. The default is 64
Threshold -- Maximum total connections to all Web sites from anonymous accounts	Specify the maximum total number of connections to all monitored Web sites from anonymous accounts that can be open during the monitoring interval. The default is 64
Threshold -- Maximum total connections to all Web sites from non-anonymous (user) accounts	Specify the maximum total number of connections to all monitored Web sites from non-anonymous (user) accounts that can be open during the monitoring interval. The default is 64
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

HTTPConnectionUtil

Use this Knowledge Script to monitor the percentage of Web site connections being utilized. If the percentage of Web site connections being used exceeds the threshold you set, AppManager raises an event.

If you receive an event stating that the "maximum number of connections" value cannot be retrieved, specify the maximum number of connections allowed for the **Maximum connections allowed** parameter. Information about the maximum number of connections allowed on a Web site can be found in the IIS Manager.

If your Web site connections are unlimited, either use the default value or refer to the IIS documentation for information about how to calculate the total number of available connections.

If the percentage of Web site connections being used exceeds the threshold you set, AppManager raises an event. No data point is collected for utilization percentage when the Maximum Connections, taken either from IIS itself or from the **Maximum connections allowed** parameter, is 0.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web sites

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if connection utilization exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for current connections and connection utilization?	Set to **y** to collect data for charts and reports. If set to y, the script returns the number of Web site connections being used and the utilization (%). No data point is collected for the percentage of utilization when the Maximum Connections is 0. The default is n.
Threshold -- Maximum connection utilization	Specify the maximum percentage of Web site connections that can be used before AppManager raises an event. The default is 90%
Maximum connections allowed on this site	If the "maximum number of connections" value cannot be retrieved from the server, specify the maximum number of connections allowed on the Web site where this script is being run. The default is 5000 connections.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

HTTPFiles

Use this Knowledge Script to report the total number of files sent to and received from a Web site during the monitoring interval. If the number of files sent to and received from the Web site exceeds either threshold you set, AppManager raises an event.

This script supports "dynamic observation" of Web sites. Dynamically observed Web sites are new sites that AppManager for IIS has observed while monitoring your IIS servers. These sites are included in jobs, but they cannot be monitored until you discover them by running the Discovery_IIS Knowledge Script again.

If you select a subset of Web sites for the job but leave the **Dynamically observe sites at each interval?** parameter set to y, this script will still do dynamic observation, and results will be returned for all Web sites, not just the subset selected. To limit results, set the **Dynamically observe...** parameter to n.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web sites

Default Schedule

The default interval is **Every 30 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe Web sites at each interval?	Set to **y** to dynamically observe Web sites at each monitoring interval. The default is y.
Exclude Web sites (separate names with commas)	Specify the name of any site you want to exclude. You can exclude multiple sites, separated by commas with no spaces. For example: `site1,site2`. **Note** If you are not dynamically observing sites, this parameter is ignored. Also, if you run the Knowledge Script on an individual site, dynamic observation is deselected and the exclusion list is ignored.
Raise event if number of files transferred exceeds a threshold?	Set to **y** to raise events. The default is y.
Collect data for files sent and files received?	Set to **y** to collect data for charts and reports. If set to y, returns the number of files sent and received by the Web site during an interval. The default is n.
Threshold -- Maximum files received	Specify the maximum number of files that can be received by the Web site during an interval before AppManager raises an event. The default is 640 files.

Description	How to Set It
Threshold -- Maximum files sent	Specify the maximum number of files that can be sent by the Web site during an interval before AppManager raises an event. The default is 640 files.
Event severity when either threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.

HTTPNotFound

Use this Knowledge Script to monitor the number of requested pages that could not be found by the Web site during the monitoring interval. When a page cannot be found, the request generally returns an `HTTP 404` error code to the client. If the number of pages not found by the Web site exceeds the threshold you set, AppManager raises an event.

This script supports "dynamic observation" of Web sites. Dynamically observed Web sites are new sites that AppManager for IIS has observed while monitoring your IIS servers. These sites are included in jobs, but they cannot be monitored until you discover them by running the Discovery_IIS Knowledge Script again.

If you select a subset of Web sites for the job but leave the **Dynamically observe sites at each interval?** parameter set to y, this script will still do dynamic observation, and results will be returned for all Web sites, not just the subset selected. To limit results, set the **Dynamically observe...** parameter to n.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web sites

Default Schedule

The default interval is **Every 30 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe Web sites at each interval?	Set to **y** to dynamically observe Web sites at each monitoring interval. The default is y.
Exclude Web sites (separate names with commas)	Specify the name of any sites you want to exclude. You can exclude multiple sites, separated by commas with no spaces. For example: `site1,site2`. **Note** If you are not dynamically observing sites, this parameter is ignored.
Raise event if number of "Page not Found" errors exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for number of "Page not Found" errors?	Set to **y** to collect data for charts and reports. If set to y, this script returns the number of `Page not Found` errors. The default is n.
Threshold -- Maximum number of "Page not Found" errors	Specify the maximum number of `Page not Found` errors allowed per interval before AppManager raises an event. The default is 200 errors.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

HTTPRequests

Use this Knowledge Script to monitor the total number of HTTP method requests during the monitoring interval. The following requests can be monitored: `COPY`, `DELETE`, `GET`, `HEAD`, `LOCK`, `MKCOL`, `MOVE`, `OPTIONS`, `POST`, `PROPFIND`, `PROPPATCH`, `PUT`, `SEARCH`, `TRACE`, and `UNLOCK`.

If the number of HTTP method requests exceeds the threshold you set, AppManager raises an event.

This script supports "dynamic observation" of Web sites. Dynamically observed Web sites are sites that AppManager for IIS has observed while monitoring your IIS servers. These sites are included in jobs, but they cannot be monitored until you discover them by running the Discovery_IIS Knowledge Script again.

If you select a subset of Web sites for the job but leave the **Dynamically observe sites at each interval?** parameter set to y, this script will still do dynamic observation, and results will be returned for all Web sites, not just the subset selected. To limit results, set the **Dynamically observe**... parameter to n.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web sites

Default Schedule

The default interval for this script is **Every hour**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe Web sites at each interval?	Set to **y** to dynamically observe Web sites at each monitoring interval. If set to n, only the Web sites you discovered are monitored. The default is y.
Exclude Web sites (separate names with commas)	Specify the names of any Web sites you want to exclude if you are dynamically observing Web sites. You can exclude multiple Web sites, separated by commas with no spaces. For example: `Default Web Sites,Administration Web Sites` **Note** If you are not dynamically observing Web sites, this parameter is ignored.
Raise event if number of HTTP method requests exceeds a threshold?	Set to **y** to raise events. The default is y.
Collect data for number of HTTP method requests?	Set to **y** to collect data for charts and reports. If set to y, the script returns the total number of HTTP method requests. The default is n.

Description	How to Set It
Threshold: Total... ...Copy requests ...Delete requests ...Get requests ...Head requests ...Lock requests ...Mkcol requests ...Move requests ...Options requests ...Post requests ...Propfind requests ...Proppatch requests ...Put requests ...Search requests ...Trace requests ...Unlock requests	Specify the maximum number of method requests of each type allowed before AppManager raises an event. The default is 100 requests.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

HTTPStatistics

Use this Knowledge Script to monitor the current number of connections from anonymous and non-anonymous (or user) accounts to a Web site, number of Web site connections, and percentage of Web site connections being utilized.

This Knowledge Script consolidates functionality that is also available in two separate IIS Knowledge Scripts:

- HTTPConnectionsInterval
- HTTPConnectionUtil

Versions of IIS Supported

6.0 and later.

Resource Objects

Web sites

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
HTTPConnectionsInterval	Select **Yes** to check for the number of Web site connections made during the monitoring interval. The default is Yes.
Dynamically observe Web sites at each interval?	Select **Yes** to dynamically observe new Web sites at each monitoring interval. The default is Yes.
Exclude Web sites (separate names with commas)	Specify the name of any request you want to exclude. You can exclude multiple sites, separated by commas with no spaces. For example: `site1,site2`. Specify "_Total" to disable monitoring of totals for all sites. **Note** If you are not dynamically observing sites, you can ignore this parameter.
Raise event if number of connections exceeds any threshold?	Select **Yes** to raise events.The default is Yes.
Collect data for number of connections per site and total per server?	Select **Yes** to collect data for charts and reports. If set to Yes, returns the number of Web server connections during the monitoring interval. The default is No.
Threshold -- Maximum connections to Web site from anonymous accounts	Specify the maximum number of Web site connections from anonymous accounts open during the monitoring interval. The default is 64.
Threshold -- Maximum connections to Web site from non-anonymous (user) accounts	Specify the maximum number of Web site connections from non-anonymous (user) accounts open during the monitoring interval. The default is 64.

Description	How to Set It
Threshold -- Maximum total connections to all Web sites from anonymous accounts	Specify the maximum total number of connections to all monitored Web sites from anonymous accounts open during the monitoring interval. The default is 64.
Threshold -- Maximum total connections to all Web sites from non-anonymous (user) accounts	Specify the maximum total number of connections to all monitored Web sites from non-anonymous (user) accounts open during the monitoring interval. The default is 64.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 12.
HTTPConnectionUtil	Select **Yes** to check for the percentage of Web site connections being utilized. The default is Yes.
Raise event if connection utilization exceeds threshold?	Select **Yes** to raise events. The default is Yes.
Collect data for current connections and connection utilization?	Select **Yes** to collect data for charts and reports. If set to Yes, the script returns the number of Web site connections being used and the utilization (%). No data point is collected for the percentage of utilization when the Maximum Connections is 0. The default is No.
Threshold -- Maximum connection utilization	Specify the maximum percentage of Web site connections that can be used before AppManager raises an event. The default is 90%
Maximum connections allowed on this site	If the “maximum number of connections” value cannot be retrieved from the server, specify the maximum number of connections allowed on the Web site where this script is being run. The default is 5000 connections.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 12.
Other settings	
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.

HTTPTransStat

Use this Knowledge Script to monitor the total number of bytes transferred per second and the number of bytes transferred to and from Web sites during the monitoring interval.

This Knowledge Script consolidates functionality that is also available in two separate IIS Knowledge Scripts:

- HTTPBytes
- HTTPBytesInterval

Note
Although each of these Knowledge Scripts are available individually, it is recommended that you use the HTTPTransStat Knowledge Script.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web sites

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
HTTPBytes	Select **Yes** to monitor the total number of bytes transferred per second to and from a Web site. The default is Yes.
Dynamically observe Web sites at each interval?	Select **Yes** to dynamically observe new Web sites at each monitoring interval. The default is Yes.
Exclude Web sites (separate names with commas)	Specify the name of any site you want to exclude. You can exclude multiple sites, separated by commas with no spaces. For example: `site1,site2`. **Note** If you are not dynamically observing sites, you can ignore this parameter.
Raise event if number of bytes transferred per second exceeds threshold?	Select **Yes** to raise events. The default is Yes.
Collect data for current transfer rate of bytes sent and received?	Select **Yes** to collect data for charts and reports. If set to Yes, returns the byte transfer rate for the HTTP server. The default is No.
Threshold -- Maximum bytes received per second	Specify the maximum bytes per second received by the HTTP server before AppManager raises an event. The default is 64000 bytes per second.

Description	How to Set It
Threshold -- Maximum bytes sent per second	Specify the maximum bytes per second sent by the HTTP server before AppManager raises an event. The default is 64000 bytes per second.
Event severity when either threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
HTTPBytesInterval	Select **Yes** to check the total number of files sent to and received from a Web site during the monitoring interval. The default is Yes.
Dynamically observe Web sites at each interval?	Select **Yes** to dynamically observe new Web sites at each monitoring interval. The default is Yes
Exclude Web sites (separate names with commas)	Specify the name of any site you want to exclude. You can exclude multiple sites, separated by commas with no spaces. For example: `site1,site2`. Specify "_Total" to disable monitoring of totals. **Note** If you are not dynamically observing sites, this parameter is ignored.
Raise event if number of bytes transferred exceeds any threshold?	Select **Yes** to raise events. The default is y.
Collect data for number of bytes sent and received per site and total for all sites?	Select **Yes** to collect data for charts and reports. If set to y, returns the number of bytes transferred to and from the HTTP server during the monitoring interval. The default is No.
Threshold -- Maximum bytes received by Web site	Specify the maximum number of bytes that can be received by a Web site during a monitoring interval before AppManager raises an event. The default is 64000 bytes.
Threshold -- Maximum bytes sent by Web site	Specify the maximum number of bytes that can be sent by a Web site during a monitoring interval before AppManager raises an event. The default is 64000 bytes.
Threshold -- Maximum total bytes received by all Web sites	Specify the maximum number of bytes that can be received by all monitored Web sites during a monitoring interval before AppManager raises an event. The default is 64000 bytes.
Threshold -- Maximum total bytes sent by all Web sites	Specify the maximum total number of bytes that can be sent by all monitored Web sites during a monitoring interval before AppManager raises an event. The default is 64000 bytes.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Other settings	
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.

IsolatedApps

This Knowledge Script monitors the number of isolated applications defined within a Web site. An "isolated" application is an application that runs out-of-process, or in a separate memory space, from the Web server. If the number of isolated applications exceeds the threshold you set, AppManager raises an event.

In IIS 6.0, IIS 5.0 isolation mode is available to support IIS 5.0 applications on IIS 6.0. However, IIS 7.0 and IIS 7.5 do not have an IIS 5.0 isolation mode, so the AppIsolated property is deprecated. All applications will run from the application pool.

Note
In IIS 6.0, by default all the applications are worker process isolation (Pooled-process). Applications will only run in in-process mode if a list of ISAPI filters and extensions for those applications are specified in the InProcessISapiApps Metabase Property. For more information, see the following Microsoft TechNet article: http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/0b8cb780-ed85-44fa-9e4f-8dc9ee2b3382.mspx?mfr=true

The following table summarizes the data streams generated and how the data is derived, depending on the IIS version:

Data streams IIS versions	Number of in-process applications	Number of pooled-process applications	Number of out-of-process applications
IIS 6.0 in IIS 5.0 compatibility mode	Application protection = IIS process (Low). Runs under `inetinfo` process.	Application protection = pooled (Medium). Runs under a pooled `dllhost` or `aspnet_wp` process.	Application protection = High (isolated). Runs under individual `dllhost` or `aspnet_wp` processes.
IIS 6.0	The `InProcessIsapiApps Metabase Property` specifies a list of ISAPI filters and extensions that will run in-process.	Application pools: Each application pool runs under `w3wp` process.	Supports out-of-process applications for IIS 5.0 backward compatibility.

Versions of IIS Supported

6.0

Resource Objects

Web sites

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of isolated applications exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for number of isolated applications?	Set to **y** to collect data for charts and reports. If set to y, the script returns the number of isolated applications. By default, data is collected.
Threshold -- Maximum Isolated applications	Specify the maximum number of isolated applications allowed before AppManager raises an event. The default is 0 applications.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

KillTopCPUProcs

Use this Knowledge Script to monitor the CPU utilization levels of the IIS process `w3wp`. If the process exceeds the CPU utilization threshold you set, AppManager raises an event. You can also set this Knowledge Script to automatically stop a process if it exceeds the CPU utilization threshold. If events are enabled, AppManager raises an event if a process is stopped and restarted.

Versions of IIS Supported

6.0 and later.

Resource Objects

IIS servers

Default Schedule

The default interval for this script is **Regular intervals, every three minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold exceeded or if process killed and restarted?	Set to **y** to raise events. The default is y.
Kill CPU-intensive processes?	Set to **y** to automatically stop any process that exceeds the threshold. The default is y.
Threshold -- Maximum% CPU utilization	Specify the maximum percentage of CPU utilization allowed by any IIS process before AppManager raises an event. The default is 90%.
Event severity when CPU utilization threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 10.
Event severity: kill...	You can set the event severity level, from 1 to 40, to indicate the importance when attempt to stop process: • **... fails**. Specify a value that indicates a process is exceeding the threshold and AppManager for IIS cannot stop the process. The default is 10. • **... succeeds**. Specify a value that indicates a process is exceeding the threshold and AppManager for IIS has successfully stopped the process. The default is 20.

Log

Use this Knowledge Script to monitor and filter information in the IIS Web site logs. If any entries in the currently active log are found that match your filter criteria, AppManager raises an event.

The specific types of information posted to the IIS Web site logs depend on how the IIS log is configured.

This script can be resource-intensive if the IIS log size is large.

The following log formats are supported:

- Microsoft's IIS Log format
- W3C Extended Log file format
- NCSA Common Log file format

All logs must use the Daily log schedule.

Notes

- The search and filter parameters only work if the log fields you select are available in the log. Make sure you select those fields for inclusion in the log being searched.
- If you are using the Log Knowledge Script with centralized binary logging enabled in IIS, then IIS will not update the individual log files of each Web site. Instead, IIS will update the centralized log file. In that case, the Log Knowledge Script does not raise events properly, and AppManager will raise an event about this situation. For best results, disable centralized binary logging in IIS.

To disable centralized binary logging for all Web sites on a server running IIS:

1. From the **Start** menu, click **Run**.
2. In the **Open** field, type the following: `<SystemDrive>\Windows\System32\cscript.exe <SystemDrive>\inetpub\AdminScripts\adsutil.vbs SET W3SVC/CentralBinaryLoggingEnabled false`
3. Click **OK**.
4. From the command prompt, type `net stop W3SVC` and press **Enter** to stop the World Wide Web Publishing Service (WWW service).
5. The WWW service must be stopped and restarted for changes to take effect.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web sites

Default Schedule

The default interval for this script is **Once daily**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if log entries match search criteria?	Set to **y** to raise events. The default is y.
Event severity when search criteria met	Set the event severity level, from 1 to 40, to indicate the importance of the event. Adjust the severity depending on which types of events you are checking for. The default is 8.
Raise event if IIS centralized logging is enabled?	Set to **y** to raise an event if centralized logging is enabled. If you use this script with centralized logging enabled, then IIS will not update the individual log files of each Web site. The default is n.
Event severity when centralized logging is enabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which centralized logging enabled. The default is 15.
Collect data for matching log entries?	Set to **y** to collect data for charts and reports. If set to y, returns the number of matched entries during the interval. The default is n.
Filter: Bytes received greater than	Specify the number of bytes received that you want to search for in the IIS log file. Numbers in these fields are “greater than” values. For example, if you specify `200` for “bytes received”, this script searches the Bytes Received column for values greater than 200. The default is 200 bytes received.
Filter: Bytes sent greater than	Specify the number of bytes sent that you want to search for in the IIS log file. Numbers in these fields are “greater than” values.
Filter: Client IP	Specify the Web address or IP address to search for in the IIS Web site log.
Filter: Client cookie	Specify the name of the client cookie to search for.
Filter: Operation type	Specify the operation type to search for. For example, type `get` or `post`. Specify one type.
Filter: Protocol status	Specify the HTTP protocol status code to search for. For example, `200`.
Filter: Protocol version	Specify the protocol version number to search for. For example, HTTP 1.0.
Filter: Referrer page	Specify the name of the referrer site to search for. The referrer site is the Web site last visited by a user.
Filter: Server IP	Specify the IP address of the server to search for.
Filter: Server name	Specify the name of the server to search for.
Filter: Time taken greater than	Specify the length of time an HTTP action (for example, `get` or `post`) took to complete. Numbers in this field are “greater than” values. For example, if you specify `200`, this script searches the Time Taken column for values greater than 200. The default is 200 milliseconds (ms).
Filter: Username	Specify the name of the user to search for.
Filter: Win32 status	Specify the Windows status code to search for. For example, `200`.

MemoryHigh

Use this Knowledge Script to detect whether an IIS application process is using too much memory. This script monitors the memory utilization and the paged and nonpaged memory pool sizes of IIS application processes.

AppManager raises an event if an instance of an application process exceeds the memory utilization threshold or either of the memory pool size thresholds.

You can select which processes to monitor. The processes to monitor depend on the version of IIS you are running.

IIS 6.0:

- `inetinfo`
- `w3wp`

IIS 7.0 and IIS 7.5:

- `inetinfo` (with IIS 6.0 compatibility option enabled)
- `w3wp`

Versions of IIS Supported

6.0 and later.

Resource Objects

IIS servers

Default Schedule

The default interval is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if any threshold exceeded?	Set to **y** to raise events. The default is y.
Collect data for memory utilization or memory pool size?	Set to **y** to collect data for charts and reports. If set to y, returns the memory utilization and memory pool sizes of the named IIS application process (in bytes). The default is n.
Process names (separated by commas)	Specify the names of the application processes to monitor. Separate multiple entries with a comma. Do not use spaces. For example: `inetinfo,dllhost`.
Threshold -- Working set size	Specify the maximum amount of memory that any instance of the selected process can use before AppManager raises an event. The default is 10,000,000 bytes.
Threshold -- Paged memory pool size	Specify the maximum size the paged memory pool that any instance of the selected process can reach before AppManager raises an event. The default is 5,000,000 bytes.

Description	How to Set It
Threshold -- Non-paged memory pool size	Specify the maximum size the non-paged memory pool that any instance of the selected process can reach before AppManager raises an event. The default is 5,000,000 bytes.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

NNTPArticles

Use this Knowledge Script to monitor the number of articles processed by an NNTP (Network News Transfer Protocol) site during the monitoring interval. If the number of articles sent and received exceeds the threshold you set, AppManager raises an event.

Note
The IIS 7.0 and 7.5 environments do not support this Knowledge Script.

Versions of IIS Supported

6.0.

Resource Objects

NNTP sites

Default Schedule

The default interval is **Every 30 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of articles transferred exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for articles received and articles sent?	Set to **y** to collect data for charts and reports. If set to y, this script returns the number of articles processed by the NNTP site. The default is n.
Threshold -- Articles received	Specify the maximum number of articles that can be received during an interval before AppManager raises an event. The default is 100 articles.
Threshold -- Articles sent	Specify the maximum number of articles that can be sent during an interval before AppManager raises an event. The default is 100 articles.
Event severity when either threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

NNTPBytes

Use this Knowledge Script to monitor the current number of bytes processed by the NNTP site. If the number of bytes processed exceeds the threshold you set, AppManager raises an event.

Note
The IIS 7.0 and 7.5 environments do not support this Knowledge Script.

Versions of IIS Supported

6.0.

Resource Objects

NNTP sites

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if current byte transfer rate exceeds a threshold?	Set to **y** to raise events. The default is y.
Collect data for bytes received and bytes sent per second?	Set to **y** to collect data for charts and reports. If set to y, this script returns the number of bytes processed by the NNTP site. The default is n.
Threshold -- Maximum bytes received	Specify the maximum bytes per second that can be received by the NNTP site before AppManager raises an event. The default is 20 bytes.
Threshold -- Maximum bytes sent	Specify the maximum bytes per second that can be sent by an NNTP site before AppManager raises an event. The default is 20 bytes.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

NNTPClientCommands

Use this Knowledge Script to monitor the number of client commands processed per second by an NNTP site. You can specify the types of commands you are interested in monitoring. For example, you may want to ignore Help requests. If the number of commands of any type exceeds the threshold you set, AppManager raises an event.

Note
The IIS 7.0 and 7.5 environments do not support this Knowledge Script.

Versions of IIS Supported

6.0.

Resource Objects

NNTP sites

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold exceeded?	Set to **y** to raise events. The default is y.
Collect data for number of client commands processed/second?	Set to **y** to collect data for charts and reports. If set to y, returns the number of client commands processed by the NNTP site per second. The default is n.
Threshold -- Maximum client commands	Specify the maximum number of client commands per second that can be processed by an NNTP site before AppManager raises an event. This threshold applies to all of the commands monitored by this script. The default is 20 commands/sec.

Description	How to Set It
Monitor: ...Article commands? ...Group commands? ...Help commands? ...IHave commands? ...Newgroups commands? ...Newnews commands? ...Next commands? ...Post commands? ...Quit commands? ...Stat commands? ...Last commands? ...List commands?	Set to **y** to monitor the commands issued per second. The threshold you specified applies to all commands monitored. The default is **n** for `Group`, `Help`, `IHave`, `Newgroups`, `Newnews`, `Quit`, `Stat`, `Last`, and `List` commands. The default is **y** for `Article`, `Next`, and `Post` commands.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 16.

NNTPClientFailures

Use this Knowledge Script to monitor the number of logon failures processed per second by an NNTP site during the monitoring interval. If the number of logon failures processed per second by the NNTP site exceeds the threshold you set, AppManager raises an event.

Note
The IIS 7.0 and 7.5 environments do not support this Knowledge Script.

Versions of IIS Supported

6.0.

Resource Objects

NNTP sites

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of logon failures exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for number of logon failures?	Set to **y** to collect data for charts and reports. If set to y, returns the number of logon failures processed by the NNTP site during the monitoring interval. The default is n.
Threshold -- Maximum number of logon failures	Specify the maximum number of logon failures that can be processed by an NNTP site before AppManager raises an event. The default is 2 failures per second.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

NNTPConnections

Use this Knowledge Script to monitor the current number of connections to an NNTP site. Both inbound connections, connections to the NNTP site, and outbound connections, those initiated by the NNTP site, are monitored.

If the number of connections to the NNTP site exceeds either of the thresholds you set, AppManager raises an event.

Note
The IIS 7.0 and 7.5 environments do not support this Knowledge Script.

Versions of IIS Supported

6.0.

Resource Objects

NNTP sites

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of current connections exceeds either threshold?	Set to **y** to raise events. The default is y.
Collect data for current inbound or outbound connections?	Set to **y** to collect data for charts and reports. If set to y, this script returns the total number of current connections and current outbound connections to the NNTP site. The default is n.
Threshold -- Maximum current inbound connections	Specify the maximum number of inbound NNTP connections that are allowed before AppManager raises an event. The default is 50 connections.
Threshold -- Maximum current outbound connections	Specify the maximum number of outbound NNTP connections that are allowed before AppManager raises an event. The default is 50 connections.
Event severity when either threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

NNTPConnectionsInterval

Use this Knowledge Script to monitor the number of inbound and outbound connections on an NNTP site, and the total number of inbound and outbound connections for all monitored NNTP sites, during the monitoring interval. If the number of inbound or outbound connections exceeds the threshold, AppManager raises an event.

Note
The IIS 7.0 and 7.5 environments do not support this Knowledge Script.

Versions of IIS Supported

6.0.

Resource Objects

NNTP sites

Default Schedule

The default interval for this script is **Every 30 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of inbound or outbound connections exceeds a threshold?	Set to **y** to raise events. The default is y.
Collect data for inbound or outbound connections per site, and total per server?	Set to **y** to collect data for charts and reports. If set to y, returns the number of inbound and outbound NNTP site connections. The default is n.
Threshold -- Maximum inbound connections per site	Specify the maximum number of inbound NNTP site connections. The default is 50.
Threshold -- Maximum outbound connections per site	Specify the maximum number of outbound NNTP site connections. The default is 50.
Threshold -- Maximum total inbound connections for all sites	Specify the maximum total number of inbound connections to all NNTP sites during the monitoring interval. The default is 50.
Threshold -- Maximum total outbound connections for all sites	Specify the maximum total number of outbound connections from all NNTP sites during the monitoring interval. The default is 50.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

NNTPConnectionUtil

Use this Knowledge Script to monitor the percentage of NNTP site connections being utilized. If the percentage of NNTP connections exceeds the threshold you set, AppManager raises an event.

The percentage of connections being used is calculated from the total number of connections allowed on the NNTP site. If you receive an event stating that the "maximum number of connections" value cannot be retrieved, specify the maximum number of connections allowed for the NNTP site where you are running the Knowledge Script for the **Maximum connections allowed** parameter. Information about the maximum number of connections allowed on an NNTP site can be found in the IIS Manager.

If your NNTP site connections are unlimited, either use the default value or refer to the IIS documentation for information about how to calculate the total number of available connections.

No data point is collected for utilization percentage when the Maximum Connections, taken either from IIS itself or from the **Maximum connections allowed** parameter, is 0.

Note
The IIS 7.0 and 7.5 environments do not support this Knowledge Script.

Versions of IIS Supported

6.0.

Resource Objects

NNTP sites

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if connection utilization exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for current connections and connection utilization?	Set to **y** to collect data for charts and reports. If set to y, returns the number of NNTP site connections. No data point is collected for the percentage of utilization when the Maximum Connections is 0. The default is n.
Threshold -- Maximum connection utilization	Specify the maximum percentage of NNTP site connections that can be used before AppManager raises an event. The default is 90%
Maximum connections allowed on this site	Specify the maximum number of connections allowed on the NNTP site where this script is being run. The default is 5000 NNTP connections.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

NNTPEventLog

Use this Knowledge Script to scan the Windows System Event Log for NNTP server events matching the criteria you specify.

During the first monitoring interval, the value you specify for the **Starting point for log search...** parameter determines how far back in the log to check for matching entries. As the script continues to run at subsequent intervals, it checks for any new entries created since the last time the log was checked.

You can further restrict the types of log entries that generate an event in two ways:

- Select only certain types of events to search for, such as Warning events.
- Use the **Filter: [...]** parameters to search only for specific information, such as events associated with a specific user or computer name.

Each time this Knowledge Script runs, it checks the System Event Log for entries matching your selection criteria and raises an event if matching entries are found. The event detail message returns the text of the log entries found.

When this Knowledge Script is set to collect data, it returns the number of log entries found, and the data point detail message returns the text of the log entries.

Note
The IIS 7.0 and 7.5 environments do not support this Knowledge Script.

Versions of IIS Supported

6.0.

Resource Objects

NNTP servers

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if log entries match search criteria?	Set to **y** to raise events. The default is y.
Collect data for matching log entries?	Set to **y** to collect data for charts and reports. If set to y, this script returns the new Event Log entries that match the search criteria. The default is n.

Description	How to Set It
Starting point for log search (past *N* hours)	Set this parameter to determine which events to search for the **first** time the Knowledge Script is run. Subsequent searches begin where the last search finished. The following values are valid: • **-1**: Search all Event Log events in the entire log. During subsequent monitoring intervals, only events that occur during the interval are searched. • **0**: Search only for events that occurred during the monitoring interval; previous events are not searched. • ***N***: The number of hours to go back in the Event Log to scan for matching events. For example, type 8 to scan the last 8 hours of the Event Log for matching entries. The default is 0.
NNTP event type: Error	Set to **y** to monitor error events. The default is y. If you set the event type to n, an error Event Log entry does not raise an event, is not returned in an event detail message, and is not collected as data if the **Collect data...** parameter is set to y.
NNTP event type: Warning	Set to **y** to monitor warning events. The default is y. If you set the event type to n, a warning Event Log entry does not raise an event, is not returned in an event detail message, and is not collected as data if the **Collect data...** parameter is set to y.
NNTP event type: Information	Set to **y** to monitor information events. The default is y. If you set the event type to n, an informational Event Log entry does not raise an event, is not returned in an event detail message, and is not collected as data if the **Collect data...** parameter is set to y.
Filter: NNTP...	Specify a search string that filters the following fields in the Event Log: • **...event ID**. Specify a single event ID or a range of event IDs; separate multiple entries with commas. For example: `414,1028-3531,4015`. • **...description**. Specify a detail description or keywords in the description. A string can contain spaces, underscores, and periods; separate multiple entries with commas. The following is an example: `no domain,critical error from the Active Directory`. The search string can contain criteria used to include and exclude entries. The following syntax rules apply: • Separate include and exclude criteria with a colon (:). Strings to the left of the colon are included; strings to the right of the colon are excluded. For example, `zones,caching:primary or secondary`. • Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ`. • If you are specifying only include criteria, the colon is not necessary. For example, `primary DNS domain`. • If you are specifying only exclude criteria, start the search string with a colon. For example, `:online help`.

Description	How to Set It
Maximum number of log entries per event message	Set the maximum number of Event Log entries that can be returned in each event report. For example, if this value is set to 30 and 67 Event Log events are found, three event reports are raised, two reports containing 30 events and one report containing 7 events. The Message column on the **Events** tab in the Operator Console displays the number of events in each event report, the type of log the events are from, and the event report batch number (the sequential number of the event report). Batch numbers start at 1 for each Knowledge Script iteration. The default is 30 entries per event message.
Event severity when search criteria met	Set the event severity level, from 1 to 40, to indicate the importance of the event. Adjust the severity depending on the types of events you are checking for. The default is 8.

NNTPServerFailures

Use this Knowledge Script to monitor the number of NNTP site failures that occurred during a monitoring interval. Site failures include failures of control messages, outbound logons, moderated postings, and total outbound connections. You can set thresholds for any or all of these failure types. If the number of NNTP site failures exceeds any threshold you set, AppManager raises an event.

Note
The IIS 7.0 and 7.5 environments do not support this Knowledge Script.

Versions of IIS Supported

6.0.

Resource Objects

NNTP sites

Default Schedule

The default interval is **Every 30 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of NNTP site failures exceeds any threshold?	Set to **y** to raise events. The default is y.
Collect data for each of the failure types?	Set to **y** to collect data for charts and reports. If set to y, returns the number of each type of site failures that occurred during an interval. The default is n.
Threshold -- Maximum failed... ...control messages ...outbound logons ...moderated postings ...total outbound connections	Specify the maximum number of NNTP site failures of each type that can occur before AppManager raises an event. The default is 1 failure.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

NNTPSpaceLow

Use this Knowledge Script to monitor used and free disk space for each logical disk drive that is used as a virtual root for an NNTP site. AppManager raises an event if any drive exceeds the maximum threshold for used disk space, or fails to meet the minimum threshold for free disk space.

Note
The IIS 7.0 and 7.5 environments do not support this Knowledge Script.

Versions of IIS Supported

6.0.

Resource Objects

NNTP sites

Default Schedule

The default interval is **Once every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold is crossed?	Set to **y** to raise events. The default is y.
Collect data for free disk space and percent used disk space?	Set to **y** to collect data for charts and reports. If set to y, this script returns the amount of used and free disk space. The default is n.
Threshold -- Maximum disk utilization	Specify the maximum percentage of disk space that can be used before AppManager raises an event. The default is 95%.
Threshold -- Minimum free disk space	Specify the minimum amount of free disk space required. If the free disk space falls below this threshold, AppManager raises an event. The default is 10 MB.
Event severity when threshold crossed	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

NNTPStatistics

Use this Knowledge Script to monitor the current number of connections to NNTP server, inbound and outbound connections to the NNTP server during a monitoring interval, and percentage of NNTP connections being utilized.

This Knowledge Script consolidates functionality that is also available in three separate IIS Knowledge Scripts:

- NNTPConnections
- NNTPConnectionsInterval
- NNTPConnectionUtil

Note
The IIS 7.0 and 7.5 environments do not support this Knowledge Script.

Versions of IIS Supported

6.0.

Resource Objects

NNTP sites

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
NNTPConnections	Select **Yes** to check for the current number of connections to an NNTP site. The default is Yes.
Raise event if number of current connections exceeds either threshold?	Select **Yes** to raise events.
Collect data for current inbound or outbound connections?	Select **Yes** to collect data for charts and reports. If set to Yes, this script returns the total number of current connections and current outbound connections to the NNTP site. By default, data is collected.
Threshold -- Maximum current inbound connections	Specify the maximum number of inbound NNTP connections that are allowed before AppManager raises an event. The default is 50 connections.
Threshold -- Maximum current outbound connections	Specify the maximum number of outbound NNTP connections that are allowed before AppManager raises an event. The default is 50 connections.
Event severity when either threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

Description	How to Set It
NNTPConnectionsInterval	Select **Yes** to check for the number of inbound and outbound connections on an NNTP site and the total number of inbound and outbound connections for all monitored NNTP sites. The default is Yes.
Raise event if number of inbound or outbound connections exceeds threshold?	Select **Yes** to raise events. The default is Yes.
Collect data for inbound or outbound connections per site and total per server?	Select **Yes** to collect data for charts and reports. If set to y, returns the number of inbound and outbound NNTP site connections. The default is No.
Threshold -- Maximum inbound connections per site	Specify the maximum number of inbound NNTP site connections. The default is 50.
Threshold -- Maximum outbound connections per site	Specify the maximum number of outbound NNTP site connections. The default is 50.
Threshold -- Maximum total inbound connections for all sites	Specify the maximum total number of inbound connections to all NNTP sites during the monitoring interval. The default is 50.
Threshold -- Maximum total outbound connections for all sites	Specify the maximum total number of outbound connections from all NNTP sites during the monitoring interval. The default is 50.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
NNTPConnectionUtil	Select **Yes** to check the percentage of NNTP site connections being utilized. The default is Yes.
Raise event if connection utilization exceeds threshold?	Select **Yes** to raise events. The default is Yes.
Collect data for current connections and connection utilization?	Select **Yes** to collect data for charts and reports. If set to Yes, returns the number of NNTP site connections. No data point is collected for the percentage of utilization when the Maximum Connections is 0. The default is No.
Threshold -- Maximum connection utilization	Specify the maximum percentage of NNTP site connections before AppManager raises an event. The default is 90%.
Maximum connections allowed on this site	Specify the maximum number of connections allowed on the NNTP site where this script is being run. The default is 5000 NNTP connections.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 12.
Other settings	
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.

Report_ASPCommunicationFailure

Use this Knowledge Script to generate a report about the number of ASP communication failures. This report allows you to make a statistical analysis of the data point values, such as the average over a time period.

This report uses data collected by the ASPCommFailure Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to yes, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETApplicationRestarted

Use this Knowledge Script to generate a report about the number of ASP.NET application restarts.

This report uses data collected by the ASPNETApplicationRestarted Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETApplicationRunning

Use this Knowledge Script to generate a report about the number of running ASP.NET applications.

This report uses data collected by the ASPNETApplicationRunning Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETErrors

Use this Knowledge Script to generate a report about the total number of parser, compilation, and run-time errors associated with ASP.NET applications.

This report uses data collected by the ASPNETErrors Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETPipelineInstances

Use this Knowledge Script to generate a report about the total number of pipeline instances. This report gives you a sense for the overall performance of ASP.NET applications.

This report uses data collected by the ASPNETPipelineInstances Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETReqStat

Use this Knowledge Script to generate a report on the following:

- Number of current ASP.NET requests
- Number ASP.NET disconnected because of a communication problem
- Time taken to execute ASP.NET requests
- ASP.NET requests that are in a queue
- Number of ASP.NET requests processed per second
- Number of ASP.NET requests rejected because the queue limits were exceeded
- Wait time (in milliseconds) that an ASP.NET request waited in a queue, before processing

This report uses data collected by the ASPNETReqStat Knowledge Script.

The Report_ASPNETReqStat script consolidates functionality that is also available in seven separate IIS Knowledge Scripts:

- Report_ASPNETRequestCurrent
- Report_ASPNETRequestDisconnected
- Report_ASPNETRequestExecuteTime
- Report_ASPNETRequestQueued
- Report_ASPNETRequestRate
- Report_ASPNETRequestRejected
- Report_ASPNETRequestWaitTime

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters, as needed:

Description	How to Set It
Select which reports to run	Select **Yes** to run specific Knowledge Scripts. By default, the check boxes are selected.
Run report for Current Requests?	Select **Yes** to check for current ASP.NET requests. The default is Yes.
Run report for Disconnected Requests?	Select **Yes** to check for disconnected ASP.NET requests. The default is Yes.

Description	How to Set It
Run report for Request Execute Time?	Select **Yes** to check the time taken to execute ASP.NET requests. The default is Yes.
Run report for Queued Requests?	Select **Yes** to check for queued ASP.NET requests. The default is Yes.
Run report for Requests Processed Per Second?	Select **Yes** to check the ASP.NET request processing rate per second. The default is Yes.
Run report for Requests Rejected?	Select **Yes** to check for rejected ASP.NET requests. The default is Yes.
Run report for Request Wait Time?	Select **Yes** to check the wait time (in milliseconds) that an ASP.NET request waited in a queue before processing The default is Yes.
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** to select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)

Description	How to Set It
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom? (yes/no)	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table? (yes/no)	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card? (yes/no)	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table? (yes/no)	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart? (yes/no)	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click Browse and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click Browse and set parameters for the output folder.
Add job ID to output folder name? (yes/no)	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click Browse and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title? (yes/no)	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success? (yes/no)	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETRequestCurrent

Use this Knowledge Script to generate a report about the number of requests currently being handled by the ASP.NET Internet Server application programming interface (ISAPI). This includes those that are queued, executing, or waiting to be written to the client.

This report uses data collected by the ASPNETRequestCurrent Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETRequestDisconnected

Use this Knowledge Script to generate a report about the number of ASP.NET requests that have been disconnected because of a communication problem.

This report uses data collected by the ASPNETRequestDisconnected Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETRequestExecuteTime

Use this Knowledge Script to generate a report about the time required to execute ASP.NET requests.

This report uses data collected by the ASPNETRequestExecuteTime Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETRequestQueued

Use this Knowledge Script to generate a report about the number of ASP.NET requests currently in all queues.

This report uses data collected by the ASPNETRequestQueued Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETRequestRate

Use this Knowledge Script to generate a report about the number of ASP.NET requests processed per second.

This report uses data collected by the ASPNETRequestRate Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETRequestRejected

Use this Knowledge Script to generate a report about the number of ASP.NET requests that were rejected because one of the queue limits was exceeded.

This report uses data collected by the ASPNETRequestRejected Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETRequestWaitTime

Use this Knowledge Script to generate a report about the time (in milliseconds) that an ASP.NET request waited in a queue before being processed.

This report uses data collected by the ASPNETRequestWaitTime Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETWorkerProcessCPU

Use this Knowledge Script to generate a report about the CPU usage of the ASP.NET worker processes.

This report uses data collected by the ASPNETWorkerProcessCPU Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETWorkerProcessExcepRate

Use this Knowledge Script to generate a report about the number of exceptions thrown per second by the common language runtime (CLR) in all ASP.NET worker processes.

This report uses data collected by the ASPNETWorkerProcessExcepRate Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETWorkerProcessExceptions

Use this Knowledge Script to generate a report about the total number of exceptions thrown by the common language runtime (CLR) in all ASP.NET worker processes.

This report uses data collected by the ASPNETWorkerProcessExceptions Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETWorkerProcessMemory

Use this Knowledge Script to generate a report about the memory usage of the ASP.NET worker processes. The memory usage reported on is nonshared or "private" memory.

This report uses data collected by the ASPNETWorkerProcessMemory Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETWorkerProcessRestarted

Use this Knowledge Script to generate a report about the number of ASP.NET worker process restarts.

This report uses data collected by the ASPNETWorkerProcessRestarted Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
It is recommended that you run the report script Every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNETWorkerProcessRunning

Use this Knowledge Script to generate a report about the number of running ASP.NET worker processes.

This report uses data collected by the ASPNETWorkerProcessRunning Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPNewEventLogEntries

Use this Knowledge Script to generate a report about the number of ASP events (entries that have Active Server Pages as their Source in the Application log).

This report uses data collected by the ASPEventLog Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPQueueBusy

Use this Knowledge Script to generate a report about the number of ASP requests currently in the queue. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the ASPQueueBusy Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPRegistryChange

Use this Knowledge Script to generate a report about the number of changes to ASP registry keys. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the ASPRegistryChange Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPReqStat

Use this Knowledge Script to generate a report about the number of ASP request errors per second, different types of ASP request failures during an interval, and ASP sessions that timed out during an interval. This report uses data collected by the ASPReqStat Knowledge Script.

The Report_ASPReqStat Knowledge Script consolidates functionality that is also available in three separate IIS Knowledge Scripts:

Report_ASPRequestError

Report_ASPRequestFailed

Report_ASPSessionTimeout

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Select which reports to run	Select **Yes** to run specific Knowledge Scripts. By default, the check boxes are selected.
Run report for ASP Request Error?	Select **Yes** to generate a report for ASP request errors. The default is Yes.
Run report for ASP Request Failed?	Select **Yes** to generate a report for failed ASP requests. The default is Yes.
Run report for ASP Session Timeout?	Select **Yes** to generate a report for ASP.NET requests that timed out. The default is Yes.
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.

Description	How to Set It
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom? (yes/no)	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table? (yes/no)	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card? (yes/no)	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table? (yes/no)	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart? (yes/no)	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	.
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPRequestError

Use this Knowledge Script to generate a report about the number of ASP request errors per second. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the ASPRequestError Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** to select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPRequestFailed

Use this Knowledge Script to generate a report about the number of ASP request failures by error type. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the ASPRequestFailed Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	.
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPSessionTimeout

Use this Knowledge Script to generate a report about the number of ASP sessions that timed out during an interval. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the ASPSessionTimeout Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_ASPThroughput

Use this Knowledge Script to generate a report about the number of ASP requests processed per second. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the ASPThroughput Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_CpuUsage

Use this Knowledge Script to generate a report about the CPU usage of IIS application processes. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the CpuHigh Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_FTPBytesRate

Use this Knowledge Script to generate a report about the total number of bytes transferred per second to and from the FTP server. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the FTPBytes Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_FTPConnections

Use this Knowledge Script to generate a report about the current number of connections from anonymous and user accounts to the FTP server. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the FTPConnections Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Generate report for selected KS:	Select the Knowledge Script from the drop-down list to generate the report. You can generate the report for the individual Knowledge Script IIS_FTPConnections or the consolidated Knowledge Script IIS_FTPStatistics. By default, **IIS_FTPConnections** is selected.
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_FTPFilesTransferRate

Use this Knowledge Script to generate a report about the total number of files sent to and received from the FTP server.

This report uses data collected by the FTPFiles Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_FTPTransStat

Use this Knowledge Script to generate a report about the total number of bytes transferred per second and the total number of files sent to and received from the FTP server. This report uses data collected by the FTPTransStat Knowledge Script.

This Knowledge Script consolidates functionality that is also available in two separate IIS Knowledge Scripts:

- Report_FTPBytesRate
- Report_FTPFilesTransferRate

Note
Although each of these Knowledge Scripts are available individually, you should run the Report_FTPTransStat report.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Select which reports to run	Select **Yes** to run specific Knowledge Scripts. By default, the check boxes are selected.
Run report for FTP Bytes Rate?	Select **Yes** to generate a report for the total number of bytes transferred per second to and from the FTP server. The default is Yes.
Run report for FTP Files Transfer Rate?	Select **Yes** to generate a report for the total number of files sent to and received from the FTP server. The default is Yes.
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.

Description	How to Set It
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom? (yes/no)	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.

Description	How to Set It
Show totals on the table? (yes/no)	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card? (yes/no)	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table? (yes/no)	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart? (yes/no)	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name? (yes/no)	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title? (yes/no)	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success? (yes/no)	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_HTTPC21WebTransferRate

Use this Knowledge Script to generate a report about the total number of bytes transferred per second to and from the Web server. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the HTTPBytes Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Generate report for selected KS:	Select the Knowledge Script from the drop-down list to generate the report. You can generate the report for the individual Knowledge Script IIS_HTTPBytes or the consolidated Knowledge Script, IIS_HTTPTransStat. By default, **IIS_HTTPBytes** is selected.
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_HTTPNotFoundError

Use this Knowledge Script to generate a report about the number of requested pages that could not be found by the Web server per monitoring interval. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the HTTPNotFound Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_MemoryUsage

Use this Knowledge Script to generate a report about the number of bytes of memory being used by the specified IIS process. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the MemoryHigh Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_NNTPArticlesTransferRate

Use this Knowledge Script to generate a report about the current number of articles processed by the NNTP server. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the NNTPArticles Knowledge Script.

Note
The IIS 7.0 environment does not support this Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_NNTPBytesTransferRate

Use this Knowledge Script to generate a report about the current number of bytes processed by the NNTP server. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the NNTPBytes Knowledge Script.

Note
The IIS 7.0 environment does not support this Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	.
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_NNTPClientCommands

Use this Knowledge Script to generate a report about the number of client commands processed by the NNTP Server. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the NNTPClientCommands Knowledge Script.

Note
The IIS 7.0 environment does not support this Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_NNTPClientFailures

Use this Knowledge Script to generate a report about the number of client security request failures processed by the NNTP server. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the NNTPClientFailures Knowledge Script.

Note
The IIS 7.0 environment does not support this Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_NNTPCurrentConnections

Use this Knowledge Script to generate a report about the total number of connections to the NNTP server. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the NNTPConnections Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Generate report for selected KS:	Select the Knowledge Script from the drop-down list to generate the report. You can generate the report for the individual Knowledge Script IIS_NNTPConnections or the consolidated Knowledge Script, IIS_NNTPStatistics. By default, **IIS_NNTPConnections** is selected.
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_NNTPTransStat

Use this Knowledge Script to generate a report about the current number of articles and bytes processed by the NNTP server. This report uses data collected by the NNTPStatistics Knowledge Script.

This Knowledge Script consolidates functionality that is also available in two separate IIS Knowledge Scripts:

- Report_NNTPArticlesTransferRate
- Report_NNTPBytesTransferRate

Note
The IIS 7.0 environment does not support this Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Select which reports to run	Select **Yes** to run specific Report Knowledge Scripts. By default, the check boxes are selected.
Run report for Article Transfer Rate?	Select **Yes** to generate a report about the current number of articles processed by the NNTP server. The default is Yes.
Run report for Bytes Transfer Rate?	Select **Yes** to generate a report about the current number of bytes processed by the NNTP server. The default is Yes.
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** and select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.

Description	How to Set It
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom? (yes/no)	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table? (yes/no)	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card? (yes/no)	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.

Description	How to Set It
Include table? (yes/no)	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart? (yes/no)	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** to open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.
Add job ID to output folder name? (yes/no)	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success? (yes/no)	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_NNTPVirtualRootDiskSpace

Use this Knowledge Script to generate a report about the used and free disk space for each drive that is used as an NNTP virtual root. This report allows you to make a statistical analysis of the data point values, such as the average or maximum value over a time period.

This report uses data collected by the NNTPSpaceLow Knowledge Script.

Note
The IIS 7.0 environment does not support this Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Note
Run this script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select time range	Click **Browse** to select a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse** to select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are deviate from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the Knowledge Script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Click **Browse** and open the Chart Settings dialog box. Define the graphic properties of the charts in your report.
Select output folder	Click **Browse** and set parameters for the output folder.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to correlate a specific instance of a Knowledge Script and the corresponding report. The default is no.
Select properties	Click **Browse** and open the Report Properties dialog box. Set the properties parameters as needed.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

RestartServer

Use this Knowledge Script to stop and then restart an IIS server. Events are raised if the attempt to stop or restart a service fails or succeeds. Any services that are stopped when the job runs can also be detected and started.

Versions of IIS Supported

6.0 and later.

Resource Objects

IIS servers

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if attempt to restart fails or succeeds?	Set to **y** to raise events. The default is y.
Restart server?	Set to **y** to automatically restart the IIS server after it is stopped. Set to n to stop but not restart the server. The default is y.
Start all stopped services?	Set to **y** to automatically restart any IIS service that is stopped when the job runs. The default is n.
Event severity when attempt to restart...	Set the event severity level, from 1 to 40, to indicate the importance when auto-restart: • **... fails**. Specify a value that indicates when AppManager for IIS cannot restart the server. The default is 10. • **... succeeds**. Specify a value that indicates that AppManager for IIS has successfully restarted the server. The default is 20.

ServiceUptime

Use this Knowledge Script to monitor the uptime of Web and FTP sites or services. If the amount of time a site has been running fails to meet the minimum threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web sites and FTP sites

Default Schedule

The default interval is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if uptime fails to meet threshold?	Set to **y** to raise events. The default is y.
Collect data for Web and FTP site or service uptime?	Set to **y** to collect data for charts and reports. If set to y, returns length of time a site has been running. The default is n.
Threshold -- Minimum uptime	Specify the minimum amount of time (in seconds) that discovered Web and FTP sites must have been up to prevent an event from being raised. The default is 10000 seconds.
Event severity when threshold not met	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

SMTPBytesInterval

Use this Knowledge Script to monitor the number of bytes transferred to and from SMTP sites, and the total for all monitored SMTP sites, during a monitoring interval. If the total number of bytes received or bytes sent by a site exceeds a threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

SMTP sites

Default Schedule

The default interval is **Once every hour**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of bytes transferred exceeds any threshold?	Set to **y** to raise events. The default is y.
Collect data for number of bytes sent or received by site, and total for all sites?	Set to **y** to collect data for charts and reports. If set to y, returns the number of bytes transferred to and from the SMTP site or all monitored sites during the monitoring interval. The default is n.
Threshold -- Maximum bytes received per SMTP site	Specify the maximum number of bytes that can be received from an SMTP site during a monitoring interval before AppManager raises an event. The default is 64000 bytes.
Threshold -- Maximum bytes sent per SMTP site	Specify the maximum number of bytes that can be sent by an SMTP site during a monitoring interval before AppManager raises an event. The default is 64000 bytes.
Threshold -- Maximum bytes received for all SMTP sites	Specify the maximum number of bytes that can be received from all SMTP sites during a monitoring interval before AppManager raises an event. The default is 64000 bytes.
Threshold -- Maximum bytes sent for all SMTP sites	Specify the maximum number of bytes that can be sent by all SMTP sites during a monitoring interval before AppManager raises an event. The default is 64000 bytes.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.

SMTPConnections

Use this Knowledge Script to monitor the current number of inbound and outbound connections on an SMTP site, and the outbound connection attempts refused by remote sites. If the current number of inbound, outbound, or refused outbound connection attempts exceeds the threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

SMTP sites

Default Schedule

The default interval is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if any threshold exceeded?	Set to **y** to raise events. The default is y.
Collect data for current number of inbound, outbound, or refused connections to an SMTP site?	Set to **y** to collect data for charts and reports. If set to y, returns the number of inbound and outbound connections and refused outbound connections. The default is n.
Threshold -- Maximum current inbound connections	Specify the maximum number of inbound connections allowed before AppManager raises an event. The default is 50 connections.
Threshold -- Maximum current outbound connections	Specify the maximum number of outbound connections allowed before AppManager raises an event. The default is 50 connections.
Threshold -- Maximum refused outbound connections	Specify the maximum number of refused outbound connections allowed before AppManager raises an event. The default is 50 connections.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

SMTPConnectionsInterval

Use this Knowledge Script to monitor the number of inbound and outbound connections to and from SMTP sites, and totals for all sites, during the monitoring interval. This script returns data for individual SMTP sites and totals for all sites. If the number of connections exceeds any threshold, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

SMTP sites

Default Schedule

The default interval for this script is **Every 30 minutes**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of inbound or outbound connections exceeds a threshold?	Set to **y** to raise events. The default is y.
Collect data for inbound or outbound connections per site and total for all sites?	Set to **y** to collect data for charts and reports. If set to y, returns the number of connections per SMTP site and totals for all monitored SMTP sites. The default is n.
Threshold -- Maximum inbound connections per site	Specify the maximum number of inbound SMTP site connections that can be open before AppManager raises an event. The default is 50.
Threshold -- Maximum outbound connections per site	Specify the maximum number of outbound SMTP site connections that can be open before AppManager raises an event. The default is 50.
Threshold -- Maximum total inbound connections for all sites	Specify the total number of inbound connections to all SMTP sites during the monitoring interval before AppManager raises an event. The default is 50.
Threshold -- Maximum total outbound connections for all sites	Specify the total number of outbound connections from all SMTP sites during the monitoring interval before AppManager raises an event. The default is 50.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

SMTPConnectionUtil

Use this Knowledge Script to monitor the percentage of SMTP server connections being utilized. If the percentage of SMTP connections exceeds the threshold you set, AppManager raises an event.

The utilization percentage is calculated from the total number of connections allowed on the SMTP site being monitored. If you receive an event stating that the "maximum number of connections" value cannot be retrieved, enter the maximum number of connections allowed on the SMTP server where you are running the Knowledge Script for the **Maximum connections allowed** parameter. Information about the maximum number of connections allowed on an SMTP server can be found in the IIS Manager.

If your SMTP server connections are unlimited, either use the default value or refer to the IIS documentation for information about how to calculate the total number of available connections.

No data point is collected for utilization percentage when the Maximum Connections, taken either from IIS itself or from the **Maximum connections allowed** parameter, is 0.

Versions of IIS Supported

6.0 and later.

Resource Objects

SMTP sites

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if connection utilization exceeds threshold?	Set to **y** to raise events. The default is y.
Collect data for current connections and connection utilization?	Set to **y** to collect data for charts and reports. If set to y, returns the number of SMTP site connections and connection utilization (%). No data point is collected for the percentage of utilization when the Maximum Connections is 0. The default is n.
Threshold -- Maximum connection utilization	Specify the maximum percentage of SMTP site connections that can be used before AppManager raises an event. The default is 90%
Maximum connections allowed on this site	If the "maximum number of connections" value cannot be retrieved from the site, enter the maximum number of connections allowed on the SMTP site. The default is 5000 SMTP connections.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

SMTPMsgs

Use this Knowledge Script to monitor SMTP messages for the monitoring interval:

- Number of bytes sent and received
- Number of messages delivered to local mailboxes
- Number of inbound messages received, and
- Number of outbound messages sent

This script raises an event if a monitored value exceeds the threshold you set.

Versions of IIS Supported

6.0 and later.

Resource Objects

SMTP sites

Default Schedule

The default interval is **Once every hour**.

Note
If the schedule is set to Run once, the value returned is the current total.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if any threshold exceeded?	Set to **y** to raise events. The default is y.
Collect data for total bytes sent or received, messages received, sent, or delivered?	Set to **y** to collect data for charts and reports. If set to y, the script returns: • total number of bytes sent or received in messages • total number of inbound messages received • total number of outbound messages sent • total number of messages delivered to local mailboxes The default is n.
Threshold -- Maximum number of message bytes received	Specify the maximum number of message bytes to be received before AppManager raises an event. The default is 50,000,000 (50 million) bytes.
Threshold -- Maximum number of message bytes sent	Specify the maximum number of message bytes to be sent before AppManager raises an event. The default is 50,000,000 (50 million) bytes.
Threshold -- Maximum number of messages delivered	Specify the maximum number of messages to be delivered before AppManager raises an event. The default is 1000 messages.
Threshold -- Maximum number of messages received	Specify the maximum number of inbound messages to be received before AppManager raises an event. The default is 1000 messages.

Description	How to Set It
Threshold -- Maximum number of messages sent	Specify the maximum number of outbound messages to be delivered, received, and sent before AppManager raises an event. The default is 1000 messages.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

SMTPQueue

Use this Knowledge Script to monitor the current number of SMTP messages in local, remote, local retry, and remote retry queues. If the number of messages in any queue exceeds the threshold you set, AppManager raises an event.

Versions of IIS Supported

6.0 and later.

Resource Objects

SMTP sites

Default Schedule

The default interval is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if any threshold exceeded?	Set to **y** to raise events. The default is y.
Collect data for SMTP messages in local, remote, local retry, and remote retry queues?	Set to **y** to collect data for charts and reports. If set to y, returns the number of messages in each type of SMTP queue. The default is n.
Threshold: Maximum... ...SMTP local queue length ...SMTP local retry queue length ...SMTP remote queue length ...SMTP remote retry queue length	Specify the maximum number of messages any monitored queue can have before AppManager raises an event. The default is 50 messages.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

SMTPStatistics

Use this Knowledge Script to monitor the number of current inbound and outbound connections on an SMTP site, and outbound connection attempts refused by remote sites, inbound and outbound connections to and from the SMTP site during a monitoring interval, and percentage of SMTP connections being utilized.

This Knowledge Script consolidates functionality that is also available in three separate IIS Knowledge Scripts:

- SMTPConnections
- SMTPConnectionsInterval
- SMTPConnectionUtil

Versions of IIS Supported

6.0 and later.

Resource Objects

SMTP sites

Default Schedule

The default interval is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
SMTPConnections	Select **Yes** to check the current number of inbound and outbound connections on an SMTP site. The default is Yes.
Raise event if any threshold exceeded?	Select **Yes** to raise events. The default is Yes.
Collect data for current number of inbound, outbound, or refused connections to an SMTP site?	Select **Yes** to collect data for charts and reports. If set to Yes, returns the number of inbound and outbound connections and refused outbound connections. The default is No.
Threshold -- Maximum current inbound connections	Specify the maximum number of inbound connections allowed before AppManager raises an event. The default is 50 connections.
Threshold -- Maximum current outbound connections	Specify the maximum number of outbound connections allowed before AppManager raises an event. The default is 50 connections.
Threshold -- Maximum refused outbound connections	Specify the maximum number of refused outbound connections allowed before AppManager raises an event. The default is 50 connections.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Description	How to Set It
SMTPConnectionsInterval	Select **Yes** to check for the number of inbound and outbound connections to and from SMTP sites, and totals for all sites, during the monitoring interval. The default is Yes.
Raise event if number of inbound or outbound connections exceeds threshold?	Select **Yes** to raise events. The default is Yes.
Collect data for inbound or outbound connections per site and total for all sites?	Select **Yes** to collect data for charts and reports. If set to Yes, returns the number of connections per SMTP site and totals for all monitored SMTP sites. The default is No.
Threshold -- Maximum inbound connections per site	Specify the maximum number of inbound SMTP site connections that can be open before AppManager raises an event. The default is 50.
Threshold -- Maximum outbound connections per site	Specify the maximum number of outbound SMTP site connections that can be open before AppManager raises an event. The default is 50.
Threshold -- Maximum total inbound connections for all sites	Specify the total number of inbound connections to all SMTP sites during the monitoring interval before AppManager raises an event. The default is 50.
Threshold -- Maximum total outbound connections for all sites	Specify the total number of outbound connections from all SMTP sites during the monitoring interval before AppManager raises an event. The default is 50.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
SMTPConnectionUtil	Select **Yes** to check the percentage of SMTP server connections being utilized. The default is Yes.
Raise event if connection utilization exceeds threshold?	Select **Yes** to raise events. The default is Yes.
Collect data for current connections and connection utilization?	Select **Yes** to collect data for charts and reports. If set to Yes, returns the number of SMTP site connections and connection utilization (%). No data point is collected for the percentage of utilization when the Maximum Connections is 0. The default is No.
Threshold -- Maximum connection utilization	Specify the maximum percentage of SMTP site connections that can be used before AppManager raises an event. The default is 90%.
Maximum connections allowed on this site	If the “maximum number of connections” value cannot be retrieved from the site, enter the maximum number of connections allowed on the SMTP site. The default is 5000 SMTP connections.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 12.
Other settings	
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.

SSLCertMon

Use this Knowledge Script to identify and monitor expiration dates of valid SSL certificates running on Web servers. AppManager raises an event if any valid SSL certificate is found. AppManager also raises an event if no SSL certification is available.

Versions of IIS Supported

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise an event if any valid SSL certificate is found?	Select **Yes** to enable events. The default is Yes.
Raise an event if no valid SSL certificate is available?	Select **Yes** to raise an event if no valid SSL certificate is available. The default is Yes.
Collect data for valid SSL certificates of IIS server?	Select **Yes** to collect data for charts and reports. The default is No.
Event severity when valid SSL certificates are found	Set the event severity for valid SSL certificates found, from 1 to 40, to indicate the importance of the event. The default is 25.
Enter the number of days for SSL certificate expiration	Specify the number of days pending before expiration of the SSL certificate, from 0 to 100. This value will show only those SSL certificates whose expiration is within the number of days specified. The default value 0 will show all the valid SSL certificates on a machine.

UDDIConnections

Use this Knowledge Script to monitor the UDDI (Universal Description, Discovery, and Integration) database connection. If the collection of data from a UDDI database fails, AppManager raises an event.

Versions of IIS Supported

- 6.0 (on 32-bit computers only)
- 7.0 (on 32-bit and 64-bit computers)
- 7.5 (on 32-bit and 64-bit computers)

Resource Objects

UDDI Server

Default Schedule

The default interval is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if collection of data fails?	Select **Yes** to raise events. If data is collected, it returns the name and description of the UDDI server. The default is Yes.
Raise event if connection to the UDDI database server fails?	Select **Yes** to enable events. The default is Yes.
Event severity when UDDI database data collection/connection fails	Set the event severity level for data collection failure, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity when UDDI database data collection/connection succeeds	Set the event severity level for data collection success, from 1 to 40, to indicate the importance of the event. The default is 25.

UnloadApps

Use this Knowledge Script to unload one or more IIS Web applications from memory. Instead of restarting IIS, you can run this script to unload a select group of Web applications from memory. This script does not restart the IIS service or refresh the cache. However, property changes to unloaded applications can take effect after you reload the applications.

AppManager raises an event if an application cannot be unloaded, or if an application is successfully unloaded.

Versions of IIS Supported

6.0.

Resource Objects

Web servers

Default Schedule

By default, this script **Runs once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if unload operation succeeds or fails?	Set to y to raise an event if an application cannot be unloaded, or if an application is successfully unloaded. The default is y.
Collect data for number of applications unloaded?	Set to **y** to collect data for charts and reports. If set to y, returns the number of applications unloaded. Returns 1 if "`root`" operation completed successfully, indicating that all applications (not just one) were successfully unloaded. The default is n.
Web sites (use semicolons as separators)	Specify the names of the sites with applications that you want to unload. Use semicolons to separate multiple entries. For example: `FINANCE;SALES;HR`
Applications to unload (separate applications with commas, sites with semicolons)	Specify the names of the applications to unload. Use commas to separate multiple entries and semicolons to map applications to the sites named in the **Web sites** field. For example, to remove the following applications from the servers used as an example above: • `AcctsPay` from the Web server `FINANCE` • `COMMForce` and `CRMSuite` from the Web server `SALES` • `Talent4Hire` from the Web server `HR` specify the following: `AcctsPay;COMMForce,CRMSuite;Talent4Hire`
Event severity when unload operation fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.

WebServiceExtensions

Use this Knowledge Script to extract the Web service extensions listed on the IIS servers and their status. If extracting the Web service extensions and their status is successful or unsuccessful, AppManager raises an event. AppManager also raises an event if the IIS server is older than version 6.0.

Version Compatibility

6.0 and later.

Resource Objects

Web servers

Default Schedule

The default schedule of this script is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if version incorrect?	Select **Yes** to raise an event if the IIS server version is below 6.0.
Event severity if operation fails	Set the event severity level, from 1 to 40, to indicate the event severity if the operation fails. The default severity level is 5.
Raise event if operation succeeds?	Set the event severity level, from 1 to 40, to indicate the event severity if the operation succeeds. The default severity level is 25.

Chapter 41
Module Builder Knowledge Scripts

As the AppManager expert, you work with the custom Module Builder Knowledge Scripts created by the subject matter expert with the Module Builder Editor. These scripts allow you to monitor the processes, services, performance counters, event log events, and log files that are critical to the performance of the managed application.

Before you can run the Knowledge Scripts for your new module, install the Module Builder managed object, and then generate the custom Knowledge Scripts. For more information, see "Generating Knowledge Scripts for a New Module" on page 2430.

A separate Module Builder Knowledge Script group exists for each module you generated with the Module Builder Editor. For more information, see "Working with Module Builder Knowledge Scripts" on page 2431.

Depending on the settings you and the subject matter expert specified in the Module Builder Editor, Module Builder creates one or more of the following Knowledge Scripts:

Knowledge Script	What It Does
EventLogCheck	Monitors a set of event log events for the application.
LogFileCheck	Monitors a set of log files for the application.
PerformanceMetrics	Monitors the status of the performance counters selected for the application.
ProcessHealthCheck	Monitors the health and status of processes selected for the application.
ServiceHealthCheck	Monitors the health and status of services related to the application.
Discovery_ModuleBuilder	Discovers configurations and resources for Module Builder.

Note
To view generic Help for Module Builder Knowledge Scripts, click **Help > Help Topics**, and then go to the Knowledge Script Reference folder on the Contents tab and select the Module Builder Knowledge Scripts folder.

Generating Knowledge Scripts for a New Module

As the AppManager expert, your responsibilities begin when you receive the `.mob` file created with the Module Builder Editor by the subject matter expert. Install the ModuleBuilder managed object files on each agent, console, and repository computer. For more information, see "Installing the Module Builder Managed Object" on page 8.

After reviewing the `.mob` file in the Module Builder Editor and making any changes needed to the settings and conditions, use the `.mob` file to generate the new module and its Knowledge Scripts.

The generation process also creates an application monitoring contract, a PDF file that describes the Windows components and settings specified by the subject matter expert in the Module Builder Editor. The Knowledge Scripts and the contract can only be generated if all the relevant settings are complete, with no required settings left as *I don't know* and no required severity levels left undefined.

You need Adobe Acrobat Reader or another PDF reader application to read the PDF file, which uses the following naming convention: `ModuleBuilder-[`*`ApplicationName`*`]_Agreement.pdf`.

Notes

- You do not need to open the `.mob` file on the same computer used by the subject matter expert when the `.mob` file was created.
- Data gathered on the subject matter expert's computer is displayed in the Module Builder Editor, but no data is gathered from your computer while you are in AppManager Expert mode.

To generate scripts for a new module:

1. Double-click the `.mob` file to open the Module Builder Editor.
2. If the Module Builder Editor does not open in AppManager Expert mode, click **Show AppManager Expert Mode**.
3. Review the contents of the `.mob` file by clicking **Configure** for each component on the Review Results and Add Details pane of the Interview Summary window.
4. Where needed, update the `.mob` file if information is incorrect or missing, including places where the subject matter expert left an option set to *I don't know*. Send the file back to the subject matter expert for more information, if needed.
5. In the Generate AppManager Module pane of the Interview Summary window, click **Generate**.
6. ***If you want to change the default severity settings for all generated Knowledge Scripts***, edit the four severity levels as needed. The smaller the number, the higher the importance in AppManager.
7. ***If you want to view a list of changes made to this file***, click **View Change History**. Edits made by the subject matter expert are listed under the *changes by SME* section of the `.txt` file, while edits by the AppManager expert are listed under *changes by AME*.
8. Click **Generate Module** and select the folder where you want to place the generated scripts and the monitoring contract.

   Note
   If you are generating a module for an application you previously used with the Module Builder Editor, the Module Builder Editor will overwrite any existing Knowledge Scripts in the default folder. If you do not want to overwrite existing scripts, navigate to a different folder or click **Make New Folder**.

9. Click **OK** to close the Module Generation Complete dialog box.

Tip
If the generation process generated any errors and you want to copy the error information into another application, press **Ctrl** while you select the errors, and then press **Ctrl+C**.

10. Click **Finish**.
11. Copy the folder containing the newly generated scripts from the `\Module Builder Projects\` folder onto a shared drive or a removable drive, or email the folder and its contents to the console computer where AppManager is installed. If you are running the Module Builder Editor and AppManager on the same computer, you can skip this step.
12. On the console computer where AppManager is installed, paste the new Module Builder folder and its contents into the `\NetIQ\AppManager\qdb\kp` folder.
13. In AppManager, check in the Knowledge Scripts. For more information about checking in scripts, see the user guides for Operator Console or Control Center.
14. At this point, the Module Builder custom module functions just like any other AppManager module. You can add computers to monitor and run the discovery process as needed.

Note
If the subject matter expert makes any changes to the module settings in the ModuleBuilder Editor, launch the Module Builder Editor and generate the scripts again using the above process. Check in the new or updated Knowledge Scripts, run the discovery process again, and update any existing jobs as well.

Working with Module Builder Knowledge Scripts

The `Discovery_ModuleBuilder-[`*`ApplicationName`*`]` appears in the Discovery Knowledge Script group, where `[`*`ApplicationName`*`]` is the application name given by the subject matter expert in the Select Application process of the Module Builder Editor.

The names for custom Knowledge Scripts created with the Module Builder Editor are structured like this: `ModuleBuilder-[`*`ApplicationName`*`]_[`*`ScriptName`*`]`, where `[`*`ScriptName`*`]` is the name of the specific Knowledge Script.

The name for a Module Builder Discovery Knowledge Script is structured like this: `Discovery_ModuleBuilder-[`*`ApplicationName`*`]`.

The names of the objects in the TreeView are structured like this:
`ModuleBuilder-[ApplicationName]:[`*`ComputerName`*`]`, where `[`*`ComputerName`*`]` is the name of the computer on which the Module Builder Editor was run.

Notes

- When deploying a Module Builder Knowledge Script on one or more computers that have more than one unique Module Builder application, the script automatically associates all Module Builder application objects, not just the objects based on the script. When deploying a Module Builder script in this scenario, use the Objects tab to unselect Module Builder applications that are not applicable.
- For monitoring policies, AppManager automatically creates jobs without control over the object matching, which could lead to failure events, such as job type mismatches.
- For rule-based management groups, you cannot use the Compare Object with Name object rule because of the way in which Module Builder objects are named. The unique portion of the object name will be to the right of the colon. As a result, you must instead use a rule-based management group, such as Match Detail.

Revising an Existing Module Builder Custom Module

As the AppManager expert, you can revise the settings or Windows components selected in the Module Builder Editor if those settings are not sufficient or accurate. You can also revise the custom module when you upgrade to a newer release of the managed application.

When a subject matter expert or an AppManager expert updates a module and the AppManager expert regenerates the resulting Knowledge Scripts, the new scripts must be checked in, a new discovery must occur, and any existing jobs should be updated.

To revise an existing module:

1. Decide if you want to create a new Module Builder custom module with its own set of Knowledge Scripts and object tree in the TreeView, or if you want to use the existing application and preserve currently running jobs and existing data streams.
2. ***If you want to create a new custom module with its own set of Knowledge Scripts***, complete the following steps:
   a. Use the Module Builder Editor to specify the application and the application components to monitor.
   b. Generate the new Knowledge Scripts.
   c. In AppManager, stop and existing jobs running with the old version of the module.
   d. Check in the new scripts.
   e. Run discovery and deploy new jobs.

3. ***If you want to use the existing Knowledge Scripts***, complete the following steps:

   a. Use the Module Builder Editor to update the existing `.mob` file or simply create a new `.mob` file with the same application name as the old version.

   b. Generate the new Knowledge Scripts.

   c. In AppManager, check in the new scripts.

Note
When you revise an existing `.mob` file, if you change the **Application name** field on the Discover Application Properties dialog box for the Select Application to Manage process, you get a new object tree and a new set of Knowledge Scripts.

4. For jobs that are currently running with the previous version of the module, you need to propagate the updated Knowledge Scripts. For more information, see the "Running Monitoring Jobs" chapter of the *AppManager Operator Console User Guide*.

Using the Browse Button to Set Parameters

Some Knowledge Script parameters can only be set by clicking the **Browse (...)** button in the Value column. Clicking **Browse (...)** launches a dialog box that lists each item individually. The dialog box allows you to edit the parameter-specific settings for each item or items to be monitored. This option is also called the Knowledge Script parameter extension.

If you want to override the settings created by the subject matter expert with the Module Builder Editor, you can change the values in the Browse dialog box as needed.

Depending on the Knowledge Script parameter, you will encounter one of the following sets of options in the resulting dialog box:

- If you want to raise an event if a certain condition is met, select **Yes** in the Raise Event? column for each item in the list you want to update. Select **No** if you do not want to raise an event.
- If you want to change the default severity level, type a new severity level number in the Severity column for each item in the list you want to update.
- If you want to edit the threshold amounts or units for a process, type a new number in the Threshold column or select an option from the Unit column for each item in the list you want to update.
- If you want to edit the threshold amounts for a performance counter, specify the new amounts for each item in the list you want to update. The Unit and Scale values are listed in the dialog box, but you cannot edit these parameters.

Tip
When relevant, click **Apply default to All** to change all parameters to the value set in the Default row. The default setting for each object is determined by the settings selected by the subject matter expert in the Module Builder Editor.

EventLogCheck

This automatically generated Knowledge Script monitors a set of event log events for the application, based on the criteria set up in the Module Builder Editor. With this Knowledge Script you can track Windows event log entries that match a filtering criterion.

You can set AppManager to send an event or alert if the specified text or conditions appear in an event log, and then collect data on those events.

Notes

- The EventLogCheck script uses the local repository on the agent computer to store the last scanned information. As a result, locally stored data for a job persists unless you remove it from the agent. If you stop an existing EventLogCheck job and then restart it later, you might not receive an event, and your data stream value might be set to zero. EventLogCheck only looks for new entries based on the last time the log file was analyzed. Because the job was an existing job, the last scan time was saved on the agent computer being monitored. When the job was restarted, the last scan time was used as the starting point.
- If you change the *Scan back* parameter for an active running EventLogCheck job, you might not get an event and your data stream value could be set to zero. By default EventLogCheck will only look for new entries based upon the last time the event log was analyzed. Because the job was an existing job, the last scan time was saved on the agent computer being monitored. When the job was restarted, the last scan time was used as the starting point.

Resource Object

Event Log object

Default Schedule

The default interval for this script is every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Log	
Scan back event log N hours on first iteration	Set this parameter to control checking for the first interval (after which checking is incremental): • **-1** for all the existing entries • **N** for the past n hours (8 for the past 8 hours, 50 for the past 50 hours, etc.) • **0** for no previous entries (only search from this moment on) The default is 0. **Note** This parameter value is only used on the first iteration of the job. If you stop the job and then start it again, this parameter will not be considered.
Threshold: Maximum number of matching entries	Click **Browse (...)** and specify the threshold for the number of matching entries for each event log. The default is 1.

Description	How to Set It
Maximum number of entries per event report	Specify the maximum number of entries to be recorded in each event's detail message. If the Knowledge Script finds more entries from the log than can be put into one event message, it will return multiple events to report all the outstanding entries in the log. The default is 30 entries.
Data Collection	
Collect data for event log?	Click **Browse (...)** and select **Yes** for each event for which you want to collect data. If enabled, data collection returns the number of matches found during the monitoring period.The default is No.
Maximum number of entries in data detail	Specify the maximum number of event log entries you want to list in the data detail. The data stream value will have the total count, but this parameter will limit the number of matches that are listed in the data detail. The default is 100 entries.
Event log data stream legend	Edit the name of the legend for the event log data stream. The default text is: “Event [EVENT_DESCRIPTION]”. [EVENT_DESCRIPTION] will be substituted with the event filter description specified in the Module Builder Editor.
Event Notification	
Event Found in Event Log	
Raise event if entry is found in event log?	Click **Browse (...)** and select **Yes** for each event for which you want to raise an AppManager event when an event condition is met. The default is based on the options selected in the Module Builder Editor.
Event severity when entry is found in event log	Click **Browse (...)** and specify the event severity for each event in which an entry is found in the event log. The default severity level is based on the options selected in the Module Builder Editor.
Event message when entry is found in event log	Edit the event message text used when an entry is found in the event log. The default text is: “Event [EVENT_DESCRIPTION] was found in the [EVENT_LOG] event log”. [EVENT_DESCRIPTION] will be substituted with the event filter description specified in the Module Builder Editor, and [EVENT_LOG] will be substituted with the Windows Event Log associated with the event filter (such as Application, System, or Security).
Additional Settings	
Event Details	
Event detail format	Specify how you want the event detail information formatted. Your options include: • **HTML Table**: Displays the information in an HTML-formatted table. • **Plain Text**: Displays the information in a table that uses plain text. The default is HTML Table.
Job Timeout	
Elapsed time for job timeout	Specify the length of system inactivity that designates a job timeout. The default is 30 minutes.
Event severity when job timeout occurs	Specify the event severity, between 1 and 40, to indicate the importance of an event raised when a job timeout occurs. The default is 10.
Event message when job timeout occurs	Edit the text of the job timeout message. The default text is: “Job timeout”.

Description	How to Set It
Job Failure Event Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 10.

LogFileCheck

This automatically generated Knowledge Script monitors a set of text log files for the application, based on the criteria set up in the Module Builder Editor.

You can use this Knowledge Script to raise AppManager events or notifications for the following situations:

- If a log file is found
- If a log file is not found
- If a specified string is found in a log file

LogFileCheck can also collect data for a specified log file after the log file has been found.

Notes

- The LogFileCheck script uses the local repository on the agent computer to store the last scanned information. As a result, locally stored data for a job persists unless you remove the data from the agent. If you stop the LogFileCheck job, and then start it again later, the monitoring continues from where it left off.
- If you stop a LogFileCheck job and then restart it later, you might not receive an event, and your data stream value might be set to zero. LogFileCheck only looks for new entries based on the last time the log file was analyzed. Because the job was an existing job, the last scan time was saved on the agent computer being monitored. When the job was restarted, the last scan time was used at the starting point.

Resource Object

Log Files object

Default Schedule

The default interval for this script is every hour.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Log File Found	
Data Collection	
Collect data for log file found?	Click **Browse (...)** and select **Yes** for all log files for which you want to collect data. If enabled, data collection returns the following: • 0 - the log file is not found • 100 - the log file is found. The default is No.
Log file found data stream legend	Edit the name of the legend for the log file found data stream. The default text is: “Log File [OBJECT]”. [OBJECT] will be substituted with the name of the log file.
Event Notification	

Description	How to Set It
Log File Found	
Raise event if log file found?	Click **Browse (...)** and select **Yes** for the log files for which you want to raise an event if the log file is found. The default is based on the options selected in the Module Builder Editor.
Event severity when log file is found	Click **Browse (...)** and set the event severity for when a log file is found. The default severity level is based on the options selected in the Module Builder Editor.
Event message when log file is found	Edit the event message text used when a log file is found. The default text is: "Log File [OBJECT] was found". [OBJECT] will be substituted with the name of the log file.
Log File Not Found	
Raise event if log file is not found?	Click **Browse (...)** and select **Yes** for all the log files for which you want to raise an event if the log file is not found. The default is based on the options selected in the Module Builder Editor.
Event severity when log file is not found	Click **Browse (...)** and set the event severity for when a log file is not found. The default severity level is based on the options selected in the Module Builder Editor.
Event message when log file is not found	Edit the event message text used when a log file is not found. The default text is: "Log File [OBJECT] was not found" [OBJECT] will be substituted with the name of the log file.
String Found in Log File	
Scan entire file or files on first iteration?	Click **Browse (...)** and select **Yes** for all the log files you want Module Builder to completely scan the first time you run the this Knowledge Script. If you have a large number of log files to scan, you might want to select No to avoid any potential performance issues on the first iteration. The default is No.
Rescan updated files?	Click **Browse (...)** and select **Yes** for the log files you want to completely rescan. When set to No, each monitored log file that changes during the monitoring interval will be scanned for new entries from the last scan position. When set to Yes, the *entire* file will be rescanned for matching entries when the file changes. The default is No.
Display additional log file text with data and event?	Click **Browse (...)** and select **Yes** for all the log files for which you want to display additional log file text with data and event. The additional log file text could be the entire line of log file data that includes the search string, the rest of the line, or the surrounding characters. This option is specified in the Module Builder Editor.
Data Collection	
Collect data for string found in log file?	Click **Browse (...)** and select **Yes** for all the log files for which you want to collect data for when Module Builder finds that log file. The default is No.
Maximum number of entries in data detail	Specify the maximum number of log files you want to list in the data detail. The data stream value will have the total count, but this parameter will limit the number of matches that are listed in the data detail. The default is 100.

Description	How to Set It
String found in log file data stream legend	Edit the name of the legend for the data stream created when Module Builder finds a log file with the specified text string. The default text for the legend is: “String [SEARCH_STRING] [CASE_SENSITIVE] [REGULAR_EXPRESSION] in log file [OBJECT]”. [SEARCH_STRING] will be substituted by the search word or words specified in the Module Builder Editor. If the *Match Case* option in the Module Builder Editor was checked, [CASE_SENSITIVE] will be replaced by “Case Sensitive” in the legend. If the *Use Regular Expression* option in Module Builder is checked, [REGULAR_EXPRESSION] will be replaced by “Uses Regular Expression” in the legend. [OBJECT] will be substituted with the name of the log file.
Event Notification	
Raise event if string is found?	Click **Browse (...)** and select **Yes** for all the log files for which you want to raise an event if the search string is found. The default setting is based on the options selected in the Module Builder Editor.
Maximum number of entries in event detail	Specify the maximum number of log files you want to list in the event detail. The data stream value will have the total count, but this parameter will limit the number of matches that are listed in the event detail. The default is 100. **Note** The matches are listed from newest to oldest.
Event message when string is found	Edit the event message text used when the search string is found. The default text for the legend is: “New [SEARCH_STRING] [CASE_SENSITIVE] [REGULAR_EXPRESSION] entry was found in log file [OBJECT]”. [SEARCH_STRING] will be substituted by the search word or words specified in the Module Builder Editor. If the *Match Case* option in the Module Builder Editor was checked, [CASE_SENSITIVE] will be replaced by “Case Sensitive” in the legend. If the *Use Regular Expression* option in Module Builder is checked, [REGULAR_EXPRESSION] will be replaced by “Uses Regular Expression” in the legend. [OBJECT] will be substituted with the name of the log file.
Additional Settings	
Event Details	
Event detail format	Specify how you want the event detail information formatted. Your options are: • **HTML Table**: Displays the information in an HTML-formatted table. • **Plain Text**: Displays the information in a table that uses plain text. The default is HTML Table.
Job Timeout	
Elapsed time for job timeout	Specify the length of system inactivity that designates a job timeout. The default is 30 minutes.
Event severity when job timeout occurs	Specify the event severity for when a job timeout occurs. The default is 10.
Event message when job timeout occurs	Edit the text of the job timeout message. The default text is: “Job timeout”.
Job Failure Event Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 10.

PerformanceMetrics

This automatically generated Knowledge Script monitors a set of performance counters for the application, based on the criteria set up in the Module Builder Editor.

You can use this Knowledge Script to raise AppManager events for the following situations:

- If the specified counter exceeds a threshold
- If the specified counter falls below a threshold

PerformanceMetrics can also collect data for the specified performance counter.

Tip
To create a dynamic view based on the name of a performance counter that has special characters such as \ or % in its name, use the wildcard symbol * in place of the special character.

Resource Object

Performance Counters object

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Performance Counter	
Data Collection	
Collect data for performance counter?	Click **Browse (...)** and select **Yes** for the performance counters for which you want to collect counter value data, modified by the Scale value selected in the Module Builder Editor, where relevant. The default is No.
Performance counter data stream legend	Edit the name of the legend for the performance counter data stream. The default text is: "Performance counter [PERFORMANCE_COUNTER]". [PERFORMANCE_COUNTER] will be substituted with the name of the performance counter.
Event Notification	
Counter Exceeds Threshold	
Raise event if counter exceeds threshold?	Click **Browse (...)** and select **Yes** for all the performance counters for which you want to raise an event if the threshold is exceeded. The default setting is based on the options selected in the Module Builder Editor.
Threshold: Maximum performance counter value	Click **Browse (...)** and edit the threshold amount for the selected performance counters. The default threshold is based on the options selected in the Module Builder Editor.
Event severity when counter exceeds threshold	Click **Browse (...)** and edit the severity level for when a selected performance counter exceeds the threshold. The default severity level is based on the options selected in the Module Builder Editor.

Description	How to Set It
Event message when counter exceeds threshold	Edit the name of the legend for the performance counter data stream for when the counter exceeds the threshold. The default text is: “Performance Counter [PERFORMANCE_COUNTER] exceeds threshold”. [PERFORMANCE_COUNTER] will be substituted with the name of the performance counter.
Counter Below Threshold	
Raise event if counter falls below threshold?	Click **Browse (...)** and select **Yes** for all the performance counters for which you want to raise an event if the counter falls below the threshold. The default setting is based on the options selected in the Module Builder Editor.
Threshold: Minimum performance counter value	Click **Browse (...)** and edit the threshold amount as needed for the selected performance counters. The default threshold is based on the options selected in the Module Builder Editor.
Event severity when counter falls below threshold	Click **Browse (...)** and edit the severity level for when a selected performance counter falls below the threshold. The default severity level is based on the options selected in the Module Builder Editor.
Event message when counter falls below threshold	Edit the name of the legend for the performance counter data stream for when the counter falls below the lower threshold. The default text is: “Performance Counter [PERFORMANCE_COUNTER] falls below threshold”. [PERFORMANCE_COUNTER] will be substituted with the name of the performance counter.
Additional Settings	
Event Details	
Event detail format	Specify how you want the event detail information formatted. Your options include: • **HTML Table**: Displays the information in an HTML-formatted table. • **Plain Text**: Displays the information in a table that uses plain text. The default is HTML Table.
Job Timeout	
Elapsed time for job timeout	Specify the length of system inactivity that designates a job timeout. The default is 5 minutes.
Event severity when job timeout occurs	Specify the event severity for when a job timeout occurs. The default is 10.
Event message when job timeout occurs	Edit the text of the job timeout message. The default text is: “Job timeout”.
Job Failure Event Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 10.

ProcessHealthCheck

This automatically generated Knowledge Script monitors the status, memory usage, and CPU usage of selected processes for your application, based on the type of information gathered in the Module Builder Editor.

You can use this Knowledge Script to raise AppManager events for the following situations:

- If the process is running, not running, no longer running, or recently started
- If the process exceeds a certain level of physical memory usage
- If the process exceeds a certain level of CPU usage

ProcessHealthCheck can also collect data for the process state, for CPU usage for the process, and for memory utilization for the process.

Resource Object

Processes object or Processes folder

Default Schedule

The default interval for this script is every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Process State	
Data Collection	
Collect data for the state of the process?	Click **Browse (...)** and select **Yes** for each process for which you want to gather process state data. The default is No.
Process state data stream legend	Edit the name of the legend for the process state data stream. The default text is: “Process [OBJECT]”. [OBJECT] will be substituted with the name of the process.
Event Notification	
Process Not Running	
Raise event if process not running?	Click **Browse (...)** and select **Yes** for each process for which you want to raise an event if that process is not running. The default setting is based on the options selected in the Module Builder Editor.
Event severity when process is not running	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised if a process is not running. The default severity level is based on the options selected in the Module Builder Editor.
Event message when process is not running	Edit the existing message that displays when the job times out. The default text is: “Process [OBJECT] is not running”. [OBJECT] will be substituted with the name of the process.
Process Running	

Description	How to Set It
Raise event if process is running?	Click **Browse (...)** and select **Yes** for each process for which you want to raise an event if that process is running. The default setting is based on the options selected in the Module Builder Editor.
Event severity when process is running	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the process is running. The default severity level is based on the options selected in the Module Builder Editor.
Event message when process is running	Edit the event message text that displays when the process is running. The default text is: “Process [OBJECT] is running”. [OBJECT] will be substituted with the name of the process.
Process No Longer Running	
Raise event if process is no longer running?	Click **Browse (...)** and select **Yes** for each process for which you want to raise an event if that process has stopped running since the last script iteration. The default setting is based on the options selected in the Module Builder Editor.
Event severity when process is no longer running	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the process is no longer running. The default severity level is based on the options selected in the Module Builder Editor.
Event message when process is no longer running	Edit the event message text that displays when the process is no longer running. The default text is: “Process [OBJECT] is no longer running”. [OBJECT] will be substituted with the name of the process.
Process Recently Started	
Raise event if process was recently started?	Click **Browse (...)** and select **Yes** for each process for which you want to raise an event if that process was started since the last iteration of this script. The default setting is based on the options selected in the Module Builder Editor.
Event severity when process was recently started	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the process was recently started. The default severity level is based on the options selected in the Module Builder Editor.
Event message when process was recently started	Edit the event message text that displays when the process has recently started. The default text is: “Process [OBJECT] was recently started”. [OBJECT] will be substituted with the name of the process.
Monitor CPU Usage?	Select **Yes** to monitor the amount of CPU the process uses. The default is based on the options selected in the Module Builder Editor.
CPU usage threshold	Click **Browse (...)** and specify the level of CPU usage for each process that will raise an event. The default threshold setting is based on the options selected in the Module Builder Editor.
Data Collection	
Collect data for CPU usage?	Click **Browse (...)** and select **Yes** for each process for which you want to gather CPU usage data. The default is No.
CPU usage data stream legend	Edit the name of the legend for the CPU usage data stream. The default text is: “Process [OBJECT] CPU usage”. [OBJECT] will be substituted with the name of the process.
Data Collection for Additional Process Instances	

Description	How to Set It
Collect data for all instances of this process, or for each individual instance?	Select the instances for which you want to collect data: • **All**: Combined; collect data on all processes and generate a single data stream for each process, regardless of how many instances of that process are running. Each instance will be listed in the detail. • **Individual**: Collect data on all instances of a process individually and display data in individual data streams. • **Both**: Collect data on all instances of a process as well as each process, and generate data streams for each instance, each process, and all instances in each process combined. The default is All.
Data stream legend for CPU usage for individual instances of a process	Edit the name of the legend for the CPU usage data stream for individual instances of a process. The default text is: “Process [OBJECT]-[PID] CPU usage”. [OBJECT] will be substituted with the name of the process, and [PID] stands for the Process ID for each instance.
Event Notification	
Raise event if CPU usage exceeds threshold?	Click **Browse (...)** and select **Yes** for each process for which you want to raise an event if the CPU usage exceeds threshold. The default setting is based on the options selected in the Module Builder Editor.
Event severity when CPU usage exceeds threshold	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the CPU usage exceeds the threshold. The default severity level is based on the options selected in the Module Builder Editor.
Event message when CPU usage exceeds threshold	Edit the event message text that displays when the CPU usage exceeds the stated threshold. The default text is: “Process [OBJECT] CPU usage above threshold”. [OBJECT] will be substituted with the name of the process, and [PID] stands for the Process ID for each instance.
Notification for Additional Process Instances	
Raise events on individual instances of a process or all at once?	Select the instances for which you want to raise events: • **All**: Single event including all instances if any instance exceeds the threshold. • **Individual**: Individual events for each instance that exceeds the threshold. The default is All.
CPU usage data stream legend for individual instances of a process	Edit the name of the data stream legend for when CPU usage exceeds the threshold for individual instances of a process. The default text is: “Process [OBJECT]-[PID] CPU usage above threshold”. [OBJECT] will be substituted with the name of the process, and [PID] stands for the Process ID for each instance.
Monitor Memory Usage?	Select **Yes** to raise an event if memory usage exceeds the threshold. The default is based on the options selected in the Module Builder Editor
Memory usage threshold	Click **Browse (...)** and specify the level of memory usage for each process that will raise an event. The default is based on the options selected in the Module Builder Editor.
Data Collection	
Collect data for memory usage?	Click **Browse (...)** and select **Yes** for each process for which you want to gather memory usage data. The default is No.

Description	How to Set It
Memory usage data stream legend	Edit the name of the legend for the memory usage data stream. The default text is: “Process [OBJECT] memory usage”. [OBJECT] will be substituted with the name of the process.
Data Collection for Additional Process Instances	
Collect data for all instances of this process, or for each individual instance?	Select the instances for which you want to collect data: • **All**: Collect data on all processes and generate a single data stream for each process, regardless of how many instances of that process are running. Each instance will be listed in the detail. • **Individual**: Collect data on all instances of a process individually and display data in individual data streams. • **Both**: Collect data on all instances of a process as well as each process, and generate data streams for each instance, each process, and all instances in each process combined. The default is All.
Data stream legend for memory usage for individual instances of a process	Edit the name of the legend for the memory usage data stream for individual instances of a process. The default text is:” Process [OBJECT]-[PID] memory usage”. [OBJECT] will be substituted with the name of the process, and [PID] stands for the Process ID for each instance.
Event Notification	
Raise event if memory usage exceeds threshold?	Click **Browse (...)** and select **Yes** for each process for which you want to raise an event if the memory usage exceeds threshold. The default setting is based on the options selected in the Module Builder Editor.
Event severity when memory usage exceeds threshold	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the memory usage exceeds the threshold. The default severity level is based on the options selected in the Module Builder Editor.
Event message when memory usage exceeds threshold	Edit the event message text that displays when memory usage exceeds the threshold. The default text is: “Process [OBJECT] memory usage above threshold”. [OBJECT] will be substituted with the name of the process.
Notification for Additional Process Instances	
Raise events on individual instances of a process or all at once?	Select the instances for which you want to raise events: • **All**: Single event including all instances if any instance exceeds the threshold. • **Individual**: Individual events for each instance that exceeds the threshold. The default is All.
Memory usage data stream legend for each individual instance of a process	Edit the name of the data stream legend for when memory usage exceeds the threshold for individual instances of a process. The default text is: “Process [OBJECT]-[PID] memory usage above threshold”. [OBJECT] will be substituted with the name of the process, and [PID] stands for the Process ID for each instance.
Additional Settings	
Event Details	

Description	How to Set It
Event detail format	Specify how you want the event detail information formatted. Your options include: • **HTML Table**: Displays the information in an HTML-formatted table. • **Plain Text**: Displays the information in a table that uses plain text. The default is HTML Table.
Job Timeout	
Elapsed time for job timeout	Specify the length of system inactivity that designates a job timeout. The default is 5 minutes.
Event severity when job timeout occurs	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job times out. The default is 10.
Event message when job timeout occurs	Edit the existing message that displays when the job times out. The default text is: “Job timeout”.
Job Failure Event Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 10.

ServiceHealthCheck

This automatically generated Knowledge Script monitors the status of Windows services related to the application, based on the type of information gathered in the Module Builder Editor.

You can use this Knowledge Script to raise AppManager events for the following situations:

- If the service is started
- If the service is disabled or paused
- If the service was not found
- If the service is not running
- If the service is unresponsive or hung
- If the service shut down normally

For some of the above situations, this script can take automated actions on the service, including:

- Starting a service that is not running or that has been shut down normally
- Stopping a service that was started
- Terminating and restarting a service that is hung

ServiceHealthCheck can also collect data for the service status.

Resource Object

Services object

Default Schedule

The default interval for this script is every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Service State	
Data Collection	
Collect data for the state of the service?	Click **Browse (...)** and select **Yes** for each service for which you want to gather service state data. The default is No.
Collect data for dependent services?	Select **Yes** to gather service data for any other services that are affected by a change in the status of the selected service. The default is unselected.
Service state data stream legend	Edit the name of the legend for the service data stream. The default text is "Service [OBJECT]". [OBJECT] will be substituted with the name of the service.
Event Notification	
Service Monitor Settings	
Service Started	

Description	How to Set It
Raise event if service is started?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if that service is started. The default setting is based on the options selected in the Module Builder Editor.
Event severity when service is started	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the service is started. The default severity level is based on the options selected in the Module Builder Editor.
Event message when service is started	Edit the event message text that displays when the service is started. The default text is “[OBJECT] Service is started”. [OBJECT] will be substituted with the name of the service.
Service Disabled	
Raise event if service is disabled?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if that service is disabled. The default setting is based on the options selected in the Module Builder Editor.
Event severity when service is disabled	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the service is disabled. The default severity level is based on the options selected in the Module Builder Editor.
Event message when service is disabled	Edit the event message text that displays when the service is disabled. The default text is “[OBJECT] Service is disabled”. [OBJECT] will be substituted with the name of the service.
Service Paused	
Raise event if service is paused?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if that service is paused. The default setting is based on the options selected in the Module Builder Editor.
Event severity when service is paused	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the service is paused. The default severity level is based on the options selected in the Module Builder Editor.
Event message when service is paused	Edit the event message text that displays when the service is paused. The default text is “[OBJECT] Service is paused”. [OBJECT] will be substituted with the name of the service.
Service Not Found	
Raise event if service is not found?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if that service is not found. The default setting is based on the options selected in the Module Builder Editor.
Event severity when service is not found	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the service is not found. The default severity level is based on the options selected in the Module Builder Editor.
Event message when service is not found	Edit the event message text that displays when the service is not found. The default text is “[OBJECT] Service is not found”. [OBJECT] will be substituted with the name of the service.
Service Not Running	
Raise event if service is not running?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if that service is not running. The default setting is based on the options selected in the Module Builder Editor.
Event severity when service is not running	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the service is not running. The default severity level is based on the options selected in the Module Builder Editor.

Description	How to Set It
Event message when service is not running	Edit the event message text that displays when the service is not running. The default text is “[OBJECT] Service is not running”. [OBJECT] will be substituted with the name of the service.
Service Unresponsive	
Raise event if service is unresponsive or hung?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if that service is unresponsive or hung. The default setting is based on the options selected in the Module Builder Editor.
Number of iterations before considering service is unresponsive	Specify the number of times the script should run without getting a response from the service before the script should consider the service to be unresponsive. The default is two iterations.
Event severity when service is unresponsive	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the service is unresponsive. The default severity level is based on the options selected in the Module Builder Editor.
Event message when service is unresponsive	Edit the event message text that displays when the service is unresponsive. The default text is “[OBJECT] Service is unresponsive or hung”. [OBJECT] will be substituted with the name of the service.
Service Shut Down Normally	
Raise event if service was shut down normally?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if that service was shut down normally. The default setting is based on the options selected in the Module Builder Editor.
Event severity when service was shut down normally	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the service was shut down normally. The default severity level is based on the options selected in the Module Builder Editor.
Event message when service was shut down normally	Edit the event message text that displays when the service was shut down normally. The default text is “[OBJECT] Service was shut down normally”. [OBJECT] will be substituted with the name of the service.
Service Action Options	
Service Auto-start	
Auto-start the service if found stopped?	Click **Browse (...)** and select **Yes** for each service you want to start if that service was stopped due to an error.
Auto-start the service if shut down normally?	Click **Browse (...)** and select **Yes** for each service you want to start if that service is shut down normally.
Auto-start dependent services?	Select **Yes** if you want to start any services that are affected by a change in the status of the selected service. The default is unselected.
Auto-start timeout for services?	Specify the length of the time to wait for the service to start before the auto-start option is considered timed out. The default is 30 seconds.
Raise event if auto-start successful?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if that service is started successfully.
Event severity when auto-start successful	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event when a service is started successfully.
Event message when auto-start successful	Edit the event message text that displays when the service is started correctly. The default text is “[OBJECT] Service auto-started successfully”. [OBJECT] will be substituted with the name of the service.
Raise event if auto-start failed?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if AppManager could not start the service.

Description	How to Set It
Event severity when auto-start failed	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager could not start the service.
Event message when auto-start failed	Edit the event message text that displays when AppManager could not start the service. The default text is “[OBJECT] Service auto-start failed”. [OBJECT] will be substituted with the name of the service.
Raise Event if Auto-start Disabled and Service is Down?	Select **Yes** if you want to raise an event if a service has auto-start disabled and the service is not running, so as a result, the service cannot be restarted. The default is Yes.
Event severity when auto-start disabled and service is stopped	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when a service has auto-start disabled and the service is not running.
Event message when auto-start disabled and service is stopped	Edit the event message text that displays when a service has auto-start disabled and the service is not running. The default text is “[OBJECT] Service stopped and auto-start disabled”.
Service Stop	
Stop the service if found started?	Click **Browse (...)** and select **Yes** for each service you want to stop if AppManager finds that the service has started. The default severity level is based on the options selected in the Module Builder Editor.
Stop dependent services?	Select **Yes** to stop any services that are dependent on the service that AppManager found that was started. The default is unselected.
Raise event if stop successful?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if that running service is stopped successfully.
Event severity when stop successful	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the service is stopped successfully.
Event message when stop successful	Edit the event message text that displays when the service is stopped successfully. The default text is “[OBJECT] Service stopped successfully”. [OBJECT] will be substituted with the name of the service.
Raise event if stop failed?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if AppManager cannot stop the service. The default is Yes.
Event severity when stop failed	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when AppManager cannot stop the service.
Event message when stop failed	Edit the event message text that displays when AppManager cannot stop the service. The default text is “[OBJECT] Service stop failed”. [OBJECT] will be substituted with the name of the service.
Terminate Service	
Terminate if service is unresponsive?	Click **Browse (...)** and select **Yes** for each service you want to stop if AppManager considers the service to be unresponsive. The default setting is based on the options selected in the Module Builder Editor.
Terminate the dependents if service is unresponsive?	Select **Yes** if you want to stop any services that are dependent on the selected service that AppManager considers to be unresponsive. The default is Yes.
Raise event if terminated successfully?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if AppManager stops the unresponsive service.
Event severity when terminate is successful	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when AppManager stops the unresponsive service.

Description	How to Set It
Event message when terminate is successful	Edit the event message text that displays when AppManager stops the unresponsive service. The default text is “[OBJECT] Service terminated successfully”. [OBJECT] will be substituted with the name of the service.
Raise event if terminate failed?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if the attempt to terminate that service failed. The default is Yes.
Event severity when terminate failed	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when AppManager cannot stop the service.
Event message when terminate failed	Edit the event message text that displays when AppManager cannot stop the service. The default text is “[OBJECT] Service termination failed”. [OBJECT] will be substituted with the name of the service.
Restart Terminated Service?	
Restart the dependents?	Select **Yes** if you want to restart any services dependent on the selected service that AppManager previously terminated. The default is Yes.
Restart timeout for services?	Specify the length of the restart timeout. The default is 30 seconds.
Raise event if service restarted successfully?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if AppManager successfully restarted that service.
Event severity when service restarted successfully	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when AppManager successfully restarted that service.
Event message when service restarted successfully	Edit the event message text that displays when AppManager successfully restarted that service. The default text is “[OBJECT] Service restarted successfully”. [OBJECT] will be substituted with the name of the service.
Raise event if service restart failed?	Click **Browse (...)** and select **Yes** for each service for which you want to raise an event if AppManager failed to restart that service. The default is Yes.
Event severity when restart failed	Click **Browse (...)** and set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when AppManager failed to restart that service.
Event message when restart failed	Edit the event message text that displays when AppManager failed to restart that service. The default text is “[OBJECT] Service failed to restart”. [OBJECT] will be substituted with the name of the service.
Additional Settings	
Event Details	
Event detail format	Specify how you want the event detail information formatted. Your options include: • **HTML Table**: Displays the information in an HTML-formatted table. • **Plain Text**: Displays the information in a table that uses plain text. The default is HTML Table.
Job Timeout	
Elapsed time for job timeout	Specify the length of system inactivity that designates a job timeout. The default is 5 minutes.
Event severity when job timeout occurs	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job times out. The default is 10.

Description	How to Set It
Event message when job timeout occurs	Edit the existing message that displays when the job times out. The default text is “Job timeout”.
Job Failure Event Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 10.

Discovery_ModuleBuilder

Use this Knowledge Script to discover all known components for your Module Builder application on your selected computer. When AppManager discovers a component for your application, that component displays as a discovered resource for management in AppManager.

Resource Object

Module Builder application

Default Schedule

The default setting for this script is to run once.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
Discovery Failure	
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the discovery job fails. The default is 5.
Partial Discovery	
Allow partial discovery?	Select **Yes** to allow a partial discovery, in which some objects were discovered successfully, but others could not be discovered.The event details for a partial discovery lists the items that were not discovered. The default is Yes.
Event severity when discovery partially succeeds	If you set this Knowledge Script to allow a partial discovery, set the event severity level for a partial discovery. The default is 15.
Successful Discovery	
Raise event if discovery fully succeeds?	Select **Yes** to raise an event when the discovery process fully succeeds, without any warnings. The default is unselected.
Event severity when discovery fully succeeds	If you set this Knowledge Script to raise an event when the job fails, set the event severity level for a failed discovery. The default is 25.
Log File	**Note** This section lists any log files selected in the Log Files component of the Module Builder Editor. If you did not define log files for monitoring, this section will not appear in the Discovery Knowledge Script parameters.
[Log File Name]	The name of each log file selected in the ModuleBuilder Editor is listed in this section, with the following two parameters associated with that log file.
Create log file object if file is not present	In the Module Builder Editor, the subject matter expert or the AppManager expert can set up conditions for a log file that currently does not exist. Select **Yes** to create the log file object even if the log file is not found during discovery. Clear this option if you do not want to create the log file object if the log file is not found. If the discovery process does not find a specified log file, a partial discovery notification is created. The default is Yes.
Log file path	Specify a new path for the location of the log file, as needed. You should modify this log file path on agent computers where the log file might be located in a different directory.

Chapter 42
MSCS Knowledge Scripts

The MSCS category provides Knowledge Scripts for monitoring Microsoft Cluster Server. These scripts can see shared drives and other shared resources from active nodes.

The Knowledge Scripts in the MSCS category are designed to run on clustered servers. They use the Cluster Administrator API, which enables them to track shared resources better.

Run the MSCS Knowledge Scripts on a server group representing all the nodes in the Microsoft Cluster Server, or on at least two different nodes. By running them on multiple nodes, you covered in case of a failure on one node, such as a computer that disconnects from the network or has a system failure. If you ran all your MSCS Knowledge Scripts on that node, you would receive no events from them.

The ability to monitor resources from active nodes applies to all the Knowledge Scripts in the MSCS category.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
EventLog	Monitors Windows Event Log entries created by the Microsoft Cluster Server (entries that have ClusSvc as their Source in the System Log).
GroupDown	Detects when a cluster resource group is not online. Can attempt to bring that cluster group online automatically.
GroupOwnerChange	Detects whether the owner of a cluster group has changed.
HealthCheck	Checks whether a node, network, resource, group, or a network interface is down. Also checks whether the ownership of a group has changed.
NetInterfaceDown	Checks whether a cluster network interface is down.
NetworkDown	Checks whether a cluster network is down.
NodeDown	Checks whether a cluster node is down.
ResourceDown	Detects when a cluster resource is not online; attempts to bring that cluster resource online automatically.
ResourceOwnerChange	Detects whether the owner of a cluster resource has changed.

EventLog

Use this Knowledge Script to monitor and filter Microsoft Windows Event Log entries created by the Microsoft Cluster Server (entries that have **ClusSvc** as their Source in the System Log). This script tracks Windows event log entries that match a set of filtering criteria and notifies you when a log entry that meets the filtering criteria is generated during the monitoring interval.

This script works on an incremental basis, meaning it does not fully rescan the event log each time it runs, and all log entries that match the filtering criteria are returned in the event or data point detail message.

Resource Object

Microsoft Cluster Server

In Windows Server 2003 environments, run this script on only one node to avoid duplication of events. Running this script on multiple nodes results in multiple scannings of the same Event Log, which in turn results in duplicate events for the same Event Log entries.

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if log entries match your search criteria. The default is y. **Note** The format for Event log entries in Windows Server 2008 differs slightly from the format of Event log entries in Windows Server 2003. This difference can affect the information displayed in an event message for events raised on failover clusters. Specifically, for Windows Server 2003, the Description in the event message is an alphabetic value derived from the ResourceName and ResourceGroup fields in the Event log. In Windows Server 2008, the Description may be a numeric value or may be blank, depending on the contents of the ResourceName and ResourceGroup fields.
Collect data?	Set to **y** to collect data for charts and reports. The default is n. If enabled, data collection returns the number of new event log entries, and the detailed message lists the log entries.
Events in past N hours	Set this parameter to control checking for the first interval (after which checking is incremental): • **-1** for all the existing entries • **n** for the past N hours (8 for the past 8 hours, 50 for the past 50 hours, etc.) • **0** for no previous entries (only search from this moment onward)
Monitor for error events?	Set to **y** to monitor the Event Log for error events. The default is y.
Monitor for warning events?	Set to **y** to monitor the Event Log for warning events. The default is y.
Monitor for information events?	Set to **y** to monitor the Event Log for information events. The default is y.

Description	How to Set It
Monitor for success audit events?	Set to **y** to monitor the Event Log for success audit events. The default is y.
Monitor for failure audit events?	Set to **y** to monitor the Event Log for failure audit events. The default is y.
Filter the Event Category field for	To monitor for events in a particular category (for example Server or Logon), enter an appropriate search string. This script looks for matching entries in the Event Log Category field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter the Event ID field for	To monitor for particular event IDs, enter an appropriate search string. This script looks for matching entries in the Event Log Event field. Multiple IDs and ranges can be entered separated by commas. For example: 1,2,10-15,202. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter the Event User field for	To monitor for events associated with a particular user, enter an appropriate search string. This script looks for matching entries in the Event Log's User field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter the Event Computer field for	To monitor for events generated by a particular computer, enter an appropriate search string. This script looks for matching entries in the Event Log Computer field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter the Event Description field for	To monitor for events with a particular detail description or containing keywords in the description, enter an appropriate search string. This script looks for matching entries in the Event Log Description field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Maximum number of entries per event report	Specify the maximum number of entries that can be recorded into each event's detail message before an event is raised. If this script finds more entries from the log than can be put into one event report, it raises multiple events to report all the outstanding entries in the log. The default is 30 entries.
Event severity level when log entries match search criteria	Set the event severity level, from 1 to 40, to indicate the importance of an event in which log entries match your search criteria. The default is 8 (red event indicator). You can adjust the severity depending on the log or type of event you are checking.
Event severity level when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the EventLog job fails unexpectedly. The default is 35 (magenta event indicator).

GroupDown

Use this Knowledge Script to detect whether a cluster resource group is online. This script raises an event if the cluster group is offline. You can set this script to automatically bring the cluster group online.

Resource Object

Microsoft cluster group

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if a cluster group is not online or if a cluster-related API failure occurs. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. The default is n. If enabled, data collection returns a value of: • **100** if the cluster resource group is online. • **50** if the group is partially online. • **0** if the cluster group is off-line. • **-1** if the cluster group cannot be found.
Auto-start cluster resource group?	Set to **y** to automatically start the cluster resource group. The default is y.
Event severity level when cluster group offline and auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster group is offline and auto-start fails. The default is 5 (red event indicator).
Event severity level when cluster group offline and auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster group is offline and auto-start succeeds. The default is 25 (blue event indicator).
Event severity level when cluster group offline and auto-start is set to n	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster group is offline and you set the *Auto-start cluster resource group?* parameter to n. The default is 18 (yellow event indicator).
Event severity level when cluster-related API failure occurs	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster-related API failure occurs. The default is 15 (yellow event indicator).

GroupOwnerChange

Use this Knowledge Script to detect whether the owner of a cluster group has changed. Changes in the ownership of a cluster group typically indicate a failover or failback operation has taken place. This script raises an event if the owner of the cluster group changes or if a cluster-related API failure occurs.

Both the event and data detail message indicate the previous cluster group owner and the new group owner.

Resource Object

Microsoft cluster group

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event when cluster group ownership changes or if a cluster-related API failure occurs. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. The default is n. If enabled, data collection returns a value of 0 if the cluster group owner has changed in the interval, or a value of 100 if the cluster group owner has stayed the same. The detail message indicates the previous group owner and the new group owner.
Event severity level when cluster group owner changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which cluster group ownership has changed. The default is 5 (red event indicator).
Event severity level when cluster-related API failure occurs	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster-related API failure occurs. The default is 15 (yellow event indicator).

HealthCheck

Use this Knowledge Script to determine whether a Microsoft Windows cluster node, network, resource, group, or network interface is down. This script can also determine whether the ownership of a cluster group has changed.

Resource Objects

Microsoft cluster node, network, resource, group, and network interface object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Collection	
Collect data?	Select **Yes** to collect data for graphs and charts. The default is Yes.
Monitoring	
Auto-start cluster resource?	Select **Yes** to automatically start a cluster resource that is down. The default is Yes.
Auto-start cluster group?	Select **Yes** to automatically start a cluster group that is down. The default is Yes.
Event Notification	
Raise event if changes occur in a network, resource, or group?	Select **Yes** to raise separate events, one for each component, for changes that occur in Cluster Server components: network, resource, or group. The default is Yes.
Raise a single event?	Select **Yes** to raise one event that summarizes all changes that have occurred in all Cluster Server components: network, resource and group. The default is Yes.
Event severity level when cluster-related API failure occurs	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster-related API failure occurs. The default is 15.
Event severity level when a node is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a node is down. The default is 8.
Network	
Event severity level when network is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the network is down. The default is 8.
Event severity level when network is partitioned	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the network is partitioned. The default is 9.
Event severity level when cluster network interface is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the cluster network interface is down. The default is 8.
Cluster Resources	

Description	How to Set It
Event severity level when cluster resource is off-line and auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster resource is offline and auto-start fails. The default is 5.
Event severity level when cluster resource is off-line and auto-start is set to 'No'	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster resource is offline and you deselected the *Auto-start cluster resource?* parameter. The default is 18.
Event severity level when cluster resource is off-line and auto-start is successful	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster resource is offline and auto-start succeeds. The default is 25.
Cluster Group	
Event severity level when cluster group owner changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which cluster group ownership has changed. The default is 5.
Event severity level when cluster group is off-line and auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster group is offline and auto-start fails. The default is 5 (red event indicator).
Event severity level when cluster group is off-line and auto-start is set to 'No'	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster group is offline and you deselected the *Auto-start cluster group?* parameter. The default is 18 (yellow event indicator).
Event severity level when cluster group is off-line and auto-start is successful	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster group is offline and auto-start succeeds. The default is 2 (blue event indicator).

NetInterfaceDown

Use this Knowledge Script to detect whether a cluster network interface is down. This script raises an event if the network interface is down or a cluster-related API failure occurs.

Resource Object

Microsoft cluster net interface object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if a cluster network interface is down or when a cluster-related API failure occurs. The default is y.
Collect data?	Set to **y** to collect data for charts and reports.The default is n. If enabled, data collection returns a value of 100 if the interface is up and a value of 0 if the interface is down.
Event severity level when cluster network interface down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster network interface is down. The default is 8 (red event indicator).
Event severity level when cluster-related API failure occurs	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster-related API failure occurs. The default is 15 (yellow event indicator).

NetworkDown

Use this Knowledge Script to detect whether a cluster network is down. This script raises an event if the network is down or if a cluster-related API failure occurs.

Resource Object

Microsoft cluster network folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the network is down, if the network has been partitioned, or when a cluster-related API failure occurs. The default is y.
Collect data?	Set to **y** to collect data for charts and reports.The default is n. If enabled, data collection returns a value of 100 if the cluster network is up and a value of 0 if the cluster network is down.
Event severity level when network down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the network is down. The default is 8 (red event indicator).
Event severity level when network has been partitioned	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the network has been partitioned. The default is 9 (red event indicator).
Event severity level when cluster-related API failure occurs	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster-related API failure occurs. The default is 15 (yellow event indicator).

NodeDown

Use this Knowledge Script to detect whether a cluster node is down. This script raises an event if the node is down or when a cluster-related API failure occurs.

Resource Object

Microsoft cluster node

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if a node is down or if a cluster-related API failure occurs. The default is y.
Collect data?	Set to **y** to collect data for charts and reports.The default is n. If enabled, data collection returns a value of 100 if the cluster node is up and a value of 0 if the cluster node is down.
Event severity level when node down	Set the event severity level, from 1 to 40, to indicate the importance o an event in which a node is down. The default is 8 (red event indicator).
Event severity level when cluster-related API failure occurs	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster-related API failure occurs. The default is 15 (yellow event indicator).

ResourceDown

Use this Knowledge Script to detect whether or not a cluster resource is online. This script raises an event if the resource if offline or if a cluster-related API failure occurs. You can set this script to attempt to bring the cluster resource online automatically.

Resource Object

Microsoft cluster resource

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if a cluster group is offline or if a cluster-related API failure occurs. The default is y.
Collect data?	Set to **y** to collect data for charts and reports.The default is n. If enabled, data collection returns a value of 100 if the cluster resource is online and a value of 0 if the cluster resource is off-line.
Auto-start cluster resource?	Set to **y** to automatically start the cluster resource. The default is y.
Event severity level when cluster group off-line and auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster group is offline and auto-start fails. The default is 5 (red event indicator).
Event severity level when cluster group off-line and auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance o an event in which a cluster group is offline and auto-start succeeds. The default is 25 (blue event indicator).
Event severity level when cluster group off-line and auto-start set to no	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster group is offline and you have set the *Auto-start cluster resource?* parameter to n. The default is 18 (yellow event indicator).
Event severity level when cluster-related API failure occurs	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a cluster-related API failure occurs. The default is 15 (yellow event indicator).

ResourceOwnerChange

Use this Knowledge Script to detect whether the owner of a cluster resource has changed. Changes in the ownership of a resource typically indicate a failover or failback operation has taken place. This script raises an event if the owner of the cluster resource changes or if a cluster-related API failure occurs.

Both the event and data detail message indicate the previous cluster resource owner and the new resource owner.

Resource Object

Microsoft cluster resource

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event is cluster resource ownership changes or when a cluster-related API failure occurs. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. The default is n. If enabled, data collection returns a value of 0 if the cluster resource owner has changed in the interval, or a value of 100 if the resource owner has stayed the same. The detail message indicates the previous resource owner and the new owner.
Event severity level when cluster resource owner changes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which cluster resource ownership has changed. The default is 5 (red event indicator).
Event severity level for cluster-related API failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which cluster-related API failure occurs. The default is 15 (yellow event indicator).

Chapter 43
NetBackupUNIX Knowledge Scripts

The NetBackupUNIX category provides the following Knowledge Scripts for monitoring NetBackup on UNIX servers.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
Clients	Monitors the number of clients managed by the NetBackup server.
DBDirSize	Monitors the size (in MB) of the NetBackup database directory on the NetBackup server.
DeviceStatus	Monitors the NetBackup device status and optionally resets.
ErrorLog	Checks for errors, generates an error log, warning, and critical entries made since the last time the script was run.
FailedJobs	Monitors the number of backup jobs that failed during the specified interval.
IncompleteJobs	Monitors the number of incomplete backup jobs during the specified interval.
LogDirSize	Monitors the size (in MB) of the NetBackup `log` directory.
PendingRequest	Monitors the number of pending device requests on the NetBackup server.
ResourceHigh	Monitors the CPU and memory usage of NetBackup daemons.
StorageUnitsChanged	Monitors whether changes are made to the storage units configured on the NetBackup Server.
SuccessfulJobs	Monitors the number of successfully completed backup jobs during the specified interval.

Clients

Use this Knowledge Script to monitor the number of NetBackup clients managed by the NetBackup server. This Knowledge Script raises an event if the number of managed clients exceeds the threshold you set.

Resource Object

NetBackup server

Default Schedule

The default interval for this Knowledge Script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event when the managed backup clients threshold is exceeded?	Set to **y** to raise events. The default is y.
Collect data for number of clients being managed?	Set to **y** to collect data for charts and reports. If set to **y**, this script returns the number of clients managed by the NetBackup server. The default is n.
Threshold -- Maximum number of clients being managed	Type a threshold for the maximum number of clients NetBackup sever can manage before raising an event. The default is 10 clients.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

DBDirSize

Use this Knowledge Script to monitor the size (in MB) of the NetBackup database directory in the NetBackup server. This Knowledge Script raises an event and executes the specified action if the size of the database directory exceeds the threshold you set.

Resource Object

NetBackup server

Default Schedule

The default interval for this Knowledge Script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event when the database directory size threshold is exceeded?	Set to **y** to raise events. The default is y.
Collect data for database directory size?	Set to **y** to collect data for charts and reports. If set to **y**, this script returns the size (in MB) of the database directory. The default is n.
Threshold -- maximum size of database directory	Type a threshold for the maximum size (in MB) of the NetBackup database directory. The default is 200 MB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.

DeviceStatus

Use this Knowledge Script to detect the status of a NetBackup device. If the device status is **Not Connected**, you can change the status to **Connected**. A NetBackup device is the medium used to store archived information, such as a tape drive.

This Knowledge Script raises an event when the auto-reset feature succeeds in resetting a device from the **Not Connected** status to the **Connected** status, and when the auto-reset feature fails.

Resource Object

NetBackup device

Default Schedule

The default interval for this Knowledge Script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Collect data for device status?	Set to **y** to collect data for charts and reports. If set to **y**, this script returns 0 if the device is down, or 100 if the device is up. The default is n.
Auto-reset device?	Set to **y** to automatically reset a device that is detected as down. The default is y.
Event severity level when auto-reset fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity level when auto-reset succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

ErrorLog

Use this Knowledge Script to generate a log of problems on the NetBackup server, and then scan the log for Error, Warning, and Critical entries.

An iteration is the schedule you set for running the Knowledge Script. For example, **Every hour**. During the first iteration, this Knowledge Script sets a starting point to check for log entries but does not generate any events. During subsequent iterations, this Knowledge Script generates events if the server creates log entries.

Resource Object

NetBackup server

Default Schedule

The default interval for this Knowledge Script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Raise event if a log entry is found?	Set to **y** to raise events. The default is y.
Collect data for the number of log entries found?	Set to **y** to collect charts for graphs and reports. If set to **y**, this script returns the total number of entries in the error log during the interval. The default is n.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.

FailedJobs

Use this Knowledge Script to monitor the number of failed backup jobs. This Knowledge Script raises an event if the number of failed jobs during the interval exceeds the set threshold.

An iteration is the schedule you set for running the Knowledge Script. For example, **Every 24 hours**. During the first iteration, this Knowledge Script sets a starting point to check for failed backup jobs but does not generate any events. During subsequent iterations, this Knowledge Script generates events if the server generates failed backup jobs.

Note
The first iteration of this Knowledge Script may list a job multiple times. In subsequent iterations, the Knowledge Script lists the jobs only once.

Resource Object

NetBackup server

Default Schedule

The default interval for this Knowledge Script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event when threshold is exceeded?	Set to **y** to raise events. The default is y.
Collect data for number of failed backup jobs?	Set to **y** to collect data for charts and reports. If set to **y**, this script returns the number of failed jobs since the last script iteration. The default is n.
Threshold -- Maximum number of failed backup jobs	Type a threshold for the maximum number of failed jobs that can be detected before an event is raised. The default is 10.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

IncompleteJobs

Use this Knowledge Script to monitor the number of incomplete backup jobs. This Knowledge Script raises an event if the number of incomplete jobs during the interval exceeds the set the threshold.

An iteration is the schedule you set for running the Knowledge Script. For example, **Every 24 hours**. During the first iteration, this Knowledge Script sets a starting point to check for incomplete backup jobs but does not generate any events. During subsequent iterations, this Knowledge Script generates events if the server generates incomplete backup jobs.

Resource Object

NetBackup server

Default Schedule

The default interval for this Knowledge Script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Raise event when the incomplete jobs threshold is exceeded?	Set to **y** to raise events. The default is y.
Collect data for number of incomplete jobs?	Set to **y** to collect data for charts and reports. If set to **y**, this script returns the number of jobs submitted and the number of incomplete jobs since the last script iteration. The default is n.
Threshold -- Maximum number of incomplete backup jobs	Type a maximum threshold for the number of incomplete jobs since the last script iteration. The default is 10.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.

LogDirSize

Use this Knowledge Script to monitor the size (in MB) of the NetBackup `log` directory. This Knowledge Script raises an event if the size of this directory exceeds the threshold you set.

Resource Object

NetBackup server

Default Schedule

The default interval for this Knowledge Script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Raise event when the log directory size threshold is exceeded?	Set to **y** to raise events. The default is y.
Collect data for log directory size?	Set to **y** to collect data for charts and reports. If set to **y**, this script returns the size (in MB) of the NetBackup `log` directory. The default is n.
Threshold -- Maximum size of `log` directory	Type a threshold for the maximum size (in MB) of the NetBackup `log` directory. The default is 200 MB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.

PendingRequest

Use this Knowledge Script to monitor the current number of pending device requests on the NetBackup server. This Knowledge Script raises an event if the current number of pending device requests exceeds the threshold you set.

Resource Object

NetBackup server

Default Schedule

The default interval for this Knowledge Script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Raise event when the current number of pending device requests threshold is exceeded?	Set to **y** to raise events. The default is y.
Collect data for number of pending device requests?	Set to **y** to collect data for charts and reports. If set to **y**, this script returns the current number of pending device requests. The default is n.
Threshold -- Maximum number of pending device requests	Type a threshold for the maximum current number of pending device requests that can be detected before an event is raised. The default is 5 requests.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

ResourceHigh

Use this Knowledge Script to monitor the CPU and memory usage of NetBackup daemons. This Knowledge Script raises an event if the CPU or memory usage exceeds the threshold you set.

Resource Objects

NetBackup daemons

Default Schedule

The default interval for this Knowledge Script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event when either threshold is exceeded?	Set to **y** to raise events. The default is y.
Collect data for CPU and memory utilization? (y/n)	Set to **y** to collect data for charts and reports. If set to **y**, returns the CPU utilization (%) and the memory utilization (MB) of the NetBackup daemons. The default is n.
Threshold -- Maximum CPU utilization	Type a threshold for the maximum CPU utilization of the NetBackup daemons (as a percentage of total CPU time) that can be detected before an event is raised. The default is 60%.
Threshold -- Maximum memory utilization	Type a threshold for the maximum number of MB of memory utilization that can be detected before an event is raised. The default is 6 MB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

StorageUnitsChanged

Use this Knowledge Script to detect whether modifications have been made to storage units configured on the NetBackup server. This Knowledge Script raises an event if you add a new storage unit or delete a storage unit.

Resource Object

NetBackup storage unit folder

Default Schedule

The default interval for this Knowledge Script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Raise event if modification to storage units is detected?	Set to **y** to raise events. The default is y.
Collect data for number of modified storage units?	Set to **y** to collect data for charts and reports. If set to **y**, this script returns the number of added and deleted storage units. The default is n.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.

SuccessfulJobs

Use this Knowledge Script to monitor the number of successfully completed backup jobs. This Knowledge Script raises an event if the number of successfully completed jobs during the interval falls below the set threshold.

An iteration is the schedule you set for running the Knowledge Script. For example, **Every 24 hours**. During the first iteration, this Knowledge Script sets a starting point to check for successful backup jobs but does not generate any events. During subsequent iterations, this Knowledge Script generates events if the server generates successful backup jobs.

Resource Object

NetBackup server

Default Schedule

The default interval for this Knowledge Script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
Raise event when threshold not met?	Set to **y** to raise events. The default is y.
Collect data for number of successfully completed backup jobs?	Set to **y** to collect data for charts and reports. If set to **y**, this script returns the number of successfully completed backup jobs since the last script iteration. The default is n.
Threshold -- Minimum number of successfully completed backup jobs	Type a minimum threshold for the number of successfully completed backup jobs since the last script iteration. The default is 10 jobs.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Example of How this Script is Used

Assume that you run three backup jobs every morning at 2 A.M. and expect all the jobs to be complete by 7 A.M. You can run this script once each day at 8 A.M. with the **Number of successfully completed jobs minimum threshold** set to **3**. This script raises an event and alerts you to possible problems if any of the scheduled backup jobs fails to complete by 8 A.M.

Chapter 44
NetBackup Knowledge Scripts

The NetBackup category provides the following Knowledge Scripts for monitoring the operations of Symantec NetBackup on Windows computers.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and pressing **F1**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What it Does
Clients	Monitors the number of clients managed by the NetBackup server.
DBDirSize	Monitors the size in MB of the NetBackup database (db) directory.
DeviceStatus	Detects when a NetBackup device is down, and optionally resets it.
ErrorLog	Scans the NetBackup error log file for Error, Warning, and Critical entries during the monitoring interval.
EventLog	Monitors the Windows Application log for entries created by NetBackup.
FailedJobs	Monitors the number of backup jobs that failed during the monitoring interval.
IncompleteJobs	Monitors the number of backup jobs that partially completed during the monitoring interval.
LogDirSize	Monitors the size (in MB) of the NetBackup log directory.
PendingRequest	Monitors the number of pending device requests on the NetBackup server.
ResourceHigh	Monitors the CPU and memory usage of NetBackup services.
ServiceDown	Monitors discovered NetBackup services to see if any service is down.
StorageUnitsChanged	Monitors whether modifications have been made to storage units configured on the NetBackup server during the monitoring interval.
SuccessfulJobs	Monitors the number of backup jobs that completed successfully during the monitoring interval.

Clients

Use this Knowledge Script to monitor the number of backup clients managed by the NetBackup server. This script raises an event if the number of clients being managed exceeds the threshold you set.

Resource Object

NetBackup server

Default Schedule

The default interval for this script is **every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if threshold exceeded?	Select **Yes** to raise an event if number of clients exceeds the threshold you set. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of clients managed by the NetBackup server. The default is unselected.
Threshold -- Maximum number of clients	Specify the maximum number of clients that can be managed by the server before an event is raise.d The default is 10 clients.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of clients exceeds the threshold you set. The default is 15.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

DBDirSize

Use this Knowledge Script to monitor the size (in MB) of the NetBackup `DB` directory. This script raises an event if the size of this directory exceeds the threshold you set.

Resource Object

NetBackup server

Default Schedule

The default interval for this script is **every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if threshold exceeded?	Select **Yes** to raise an event if the size of the DB directory exceeds the threshold you set. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the size (in MB) of the NetBackup db directory. The default is unselected.
Threshold -- Maximum size of DB directory	Specify the maximum size the the NetBackup DB directory can attain before an event is raised. The default is 20 MB.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the size of the NetBackup DB directory exceeds the threshold you set. The default is 15.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

DeviceStatus

Use this Knowledge Script to detect when a NetBackup tape device is `DOWN`, and optionally set it to an `UP` state. This script raises an event when the reset feature succeeds in resetting a device from the `DOWN` state to the `UP` state, and when the reset feature fails.

Resource Object

NetBackup device

Default Schedule

The default interval for this script is **every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if device is down?	Select **Yes** to raise an event if the device is down. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns 0 if the device is down, or 100 if the device is up. The default is unselected.
Reset device?	Select **Yes** to automatically reset a device that is detected as down. The default is unselected.
Event severity when reset fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager fails to reset a device. The default is 10.
Event severity when reset succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager succeeds in resetting a device. The default is 25.
Event severity when device is down and reset is not enabled	Set the event severity level, from 1 to 40, to indicate the importance of the event when the device is down and the *Reset device?* parameter is disabled. The default severity level is 20.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

ErrorLog

Use this Knowledge Script to generate a log of problems on the NetBackup server, and then scan that log for Error, Warning, and Critical entries. The first iteration of the script collects all entries for the last 24 hours. Subsequent iterations of the script collect entries made since the previous iteration. This script raises an event if the number of entries exceeds the threshold you set.

Note
When running this script on a media server, AppManager filters log entries and only collects entries originating from that media server. No filtering is applied when running this script on a master server, so AppManager returns log entries originating from both the master server and/or any associated media servers.

Resource Object

NetBackup server

Default Schedule

The default interval for this script is **every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if threshold exceeded?	Select **Yes** to raise an event if the number of error entries exceeds the threshold you set. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of entries in the error log during the monitoring interval. The default is unselected.
Threshold--Maximum number of error entries	Specify the maximum number of entries that can be found during the monitoring interval before an event is raised. The default is 0.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of error entries exceeds the threshold you set. The default is 15.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

EventLog

Use this Knowledge Script to monitor event log entries created by NetBackup. These entries are under the Windows Application Log. You can define other categories for filtering Application Log entries, such as event ID and event description.

Resource Object

NetBackup server

Default Schedule

The default interval for this script is **every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if threshold exceeded?	Select **Yes** to raise an event if the number of log entries exceeds the threshold you set. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of log entries that match the search criteria. The default is unselected.
Start collecting events from past N hours	Use this parameter to determine which events are searched the first time you run the Knowledge Script job. Subsequent searches begin where the previous one finished. The following entries are valid: • **-1** to search all existing log entries during the first interval • ***N*** to search entries for the past *N* hours (8 for the past 8 hours, 50 for the past 50 hours, etc.) • **0** to search no previous entries (search from the current time forward) The default is 0.
Threshold -- Maximum number of log entries	Specify the maximum number of new log entries that can be found during the monitoring interval before an event is raised. The default is 10.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of log entries exceeds the threshold you set. The default is 15.
Log Entry Selection	
Count ERROR entries	Select **Yes** to monitor this type of event. The default is Yes..
Count WARNING entries	Select **Yes** to monitor this type of event. The default is Yes..
Count INFO entries	Select the **Yes** to monitor this type of event. The default is Yes..
Text filter for the Event ID field	Provide an appropriate search string to find matching entries in the Event field of the Event Log. Separate multiple IDs with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.

Description	How to Set It
Text filter for the Event Description field	Provide an appropriate search string to find matching entries in the Description field of the Event Log. Separate multiple strings with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

FailedJobs

Use this Knowledge Script to monitor the number of failed backup jobs. This script raises an event if the number of failed jobs during the interval exceeds the threshold you set. A failed job is one that returns an `Exit` status code of `>1` in the NetBackup log.

During the first iteration, this Knowledge Script checks for failed backup jobs during the preceding 24 hours. During subsequent iterations, this script checks for failed backup jobs during the scheduled interval. For example, if this script is set to run **every 8 Hour(s)**, then it checks for failed jobs during the previous eight hours.

Note
When running this script on a media server, AppManager filters log entries and only collects entries originating from that media server. No filtering is applied when running this script on a master server, so AppManager returns log entries originating from both the master server and any associated media servers.

Resource Object

NetBackup server

Default Schedule

The default interval for this script is **every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if threshold exceeded?	Select **Yes** to raise an event if the number of failed jobs exceeds the threshold ou set. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of failed jobs during the interval you specify. The default is unselected.
Threshold -- Maximum number of failed jobs	Specify the maximum number of failed jobs allowed during the monitoring interval before an event is raised. The default is 10.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of failed jobs exceeds the threshold you set. The default is 15.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

IncompleteJobs

Use this Knowledge Script to monitor the number of incomplete backup jobs. If the number of incomplete jobs during the interval exceeds the threshold you set, an event is raised. An incomplete job is one that returns an `Exit` status code of `=1` in the NetBackup log.

During the first iteration, this Knowledge Script checks for incomplete backup jobs during the preceding 24 hours. During subsequent iterations, this script checks for incomplete backup jobs during the scheduled interval. For example, if this script is set to run every 8 hours, it checks for incomplete jobs during the previous eight hours.

Note
When running this script on a media server, AppManager filters log entries and only collects entries originating from that media server. No filtering is applied when running this script on a master server, so AppManager returns log entries originating from both the master server and/or any associated media servers.

Resource Object

NetBackup server

Default Schedule

The default interval for this script is **every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if threshold exceeded?	Select **Yes** to raise an event if the number of incomplete jobs exceeds the threshold you set. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of jobs submitted and the number of incomplete jobs during the interval you specify. The default is unselected.
Threshold -- Maximum number of incomplete jobs	Specify the maximum number of incomplete jobs allowed during the monitoring interval before an event is raised. The default is 10.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of incomplete jobs exceeds the threshold you set. The default is 15.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

LogDirSize

Use this Knowledge Script to monitor the size (in MB) of the NetBackup log directory. This script raises an event if the size of this directory exceeds the threshold you set.

Resource Object

NetBackup server

Default Schedule

The default interval for this script is **every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if threshold exceeded?	Select **Yes** to raise an event if the size of the log directory exceeds the threshold you set. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the size (in MB) of the NetBackup log directory. The default is unselected.
Threshold -- Maximum size of log directory	Specify the maximum size the NetBackup log directory can attain before an event is raised. The default is 20 MB.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the size of the log directory exceeds the threshold you set. The default is 15.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

PendingRequest

Use this Knowledge Script to monitor the number of pending device requests on the NetBackup server. This script raises an event if the number of pending requests exceeds the threshold you set.

Resource Object

NetBackup server

Default Schedule

The default interval for this script is **every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if threshold exceeded?	Select **Yes** to raise an event if the number of pending requests exceeds the threshold you set. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of pending device requests. The default is unselected.
Threshold -- Maximum number of pending device requests	Specify the maximum number of device requests that can be pending before an event is raised. The default is 10 requests.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of pending requests exceeds the threshold you set. The default is 15.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

ResourceHigh

Use this Knowledge Script to monitor the CPU and memory utilization of NetBackup services. This script raises an event if CPU or memory utilization exceeds the thresholds you set.

Resource Object

NetBackup service

Default Schedule

The default interval for this script is **every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if threshold exceeded?	Select **Yes** to raise an event if CPU usage or memory utilization exceeds the threshold you set. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of CPU usage and the number of MB of memory usage for a service. The default is unselected.
Threshold -- Maximum percent CPU usage	Specify the maximum amount of CPU usage allowed before an event is raised. The default is 60%.
Threshold -- Maximum memory usage	Specify the maximum memory usage allowed before an event is raised. The default is 6 MB.
Event severity when CPU or memory threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage or memory utilization exceeds the threshold you set. The default is 15.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

ServiceDown

Use this Knowledge Script to monitor discovered NetBackup services to see if any service is down. This script raises an event if a service is not running. This script can automatically restart any service that is down.

Resource Object

NetBackup service

Default Schedule

The default interval for this script is **every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if service is down?	Select **Yes** to raise an event if a service is down. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns: • 100--monitored service is running • 0--monitored service is not running. The default is unselected.
Restart service?	Select **Yes** to automatically restart any service that is down. The default is Yes.
Event severity when...	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an attempt is made to restart a service that is down, and: • **... restart fails**. Specify a value that indicates the service is down and AppManager for Symantec NetBackup cannot restart it. The default is 10. • **... restart succeeds**. Specify a value that indicates the service was down and AppManager for Symantec NetBackup successfully restarted it. The default is 25. • **... service is down and restart is not enabled**. Specify a value to indicate the service is down and the *Restart service?* parameter is disabled. The default is 20.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

StorageUnitsChanged

Use this Knowledge Script to monitor whether modifications have been made to storage units configured on the NetBackup server during the monitoring interval. This script raises an event if a storage unit is deleted or a new one is added.

Resource Object

NetBackup storage unit folder

Default Schedule

The default interval for this script is **every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if storage units are changed?	Select **Yes** to raise an event if a storage unit has been modified. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of added and deleted storage units. The default is unselected.
Event severity when a storage unit is changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a storage unit has been modified. The default is 15.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

SuccessfulJobs

Use this Knowledge Script to monitor the number of successfully completed backup jobs. This script raises an event if the number of successfully completed jobs during the interval falls below the threshold you set. A successful job is one that returns an `Exit` status code `=0` in the NetBackup log.

During the first iteration, this Knowledge Script checks for successful backup jobs during the previous 24 hours. During subsequent iterations, this script checks for successful backup jobs during the scheduled interval. For example, if this script is set to run **every 8 Hour(s)**, then it checks for successful jobs during the previous eight hours.

The following is an example of how you can use this Knowledge Script. Assume you run three backup jobs every morning at 2:00 AM, and you expect all of the jobs to be complete by 7:00 AM. You can run this script once a day at 8:00 AM. with the *Threshold – Minimum number of successfully completed jobs* parameter set to 3. If any of the scheduled backup jobs fails to complete by 8:00 AM, an event is raised, alerting you to possible problems.

Note
When running this script on a media server, AppManager filters log entries and only collects entries originating from that media server. No filtering is applied when running this script on a master server, so AppManager returns log entries originating from both the master server and/or any associated media servers.

Resource Object

NetBackup server

Default Schedule

The default interval for this script is **every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitoring Parameters	
Raise event if threshold not met?	Select **Yes** to raise an event if the number of successfully completed jobs falls below the threshold you set. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of successfully completed backup jobs during the interval you specify. The default is unselected.
Threshold -- Minimum number of successfully completed jobs	Specify the minimum number of backup jobs that must be successfully completed to prevent an event from being raised. The default is 10 jobs.
Event severity when threshold is not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of successfully completed jobs falls below the threshold you set. The default is 15.
Success and Failure Events	
Raise event on script success?	Select **Yes** to raise an event if the Knowledge Script job succeeds. The default is unselected.

Description	How to Set It
Severity of success event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job succeeds. The default is 35.
Severity of event raised when script fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 10.

Chapter 45
NetServices Knowledge Scripts

The NetServices category provides Knowledge Scripts for monitoring network services, such as monitoring the availability and use of the Windows Internet Name Service (WINS) server. This Knowledge Script category is added when you discover Windows.

Note
You can use the NetServices category to monitor Windows Server 2008 services.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
DHCPHealthCheck	Checks the availability and SNMP MIB counter of the DHCP server.
DHCPLeases	Monitors the percentage of DHCP address leases that are being used.
DNSHealthCheck	Monitors availability, CPU usage, memory usage, and name resolution of the DNS service.
DNSSync	Checks connectivity between two DNS servers.
RASConnections	Monitors the average number of connections to the remote access server (RAS).
RASErrors	Monitors the total number of remote access server (RAS) errors in an interval.
RASHealthCheck	Checks the availability and CPU usage of the RAS server.
RASStat	Monitors the throughput of the RAS server.
WINSConflict	Monitors conflict activity on the WINS server.
WINSFailure	Reports the number of failures per second on the WINS server.
WINSHealthCheck	Checks availability and CPU usage of the WINS server.
WINSQueries	Monitors query activity on the WINS server.
WINSReplication	Monitors replication activity on the WINS server.
WINSStat	Monitors the total registrations, renewals, and releases on the WINS server.

DHCPHealthCheck

Use this Knowledge Script to check the status of the Dynamic Host Configuration Protocol (DHCP) service and the SNMP MIB variable value for a DHCP object identifier (OID). If the DHCP service is not running or a valve cannot be retrieved for the DHCP OID, an event is raised. If the DHCP service is not running, it can be automatically restarted.

Prerequisite

This script requires the Microsoft SNMP service to be running.

Resource Object

DHCP service object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event when DHCP service is down or MIB counter can't be retrieved?	Set to **y** to raise an event when the DHCP service is down or the MIB counter cannot be retrieved. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the DHCP service is running, or • **0** -- the service is not running. The default is n.
Auto-start service?	Set to **y** to automatically restart the DHCP service. The default is y.
Event severity level for service down; restart failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DHCP service is down and AppManager cannot restart the service. The default is 5 (red event indicator).
Event severity level for service down; restart successful	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DHCP service is down and AppManager successfully restarted the service. The default is 25 (blue event indicator).
Event severity level for service down; don't restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DHCP service is down and the *Auto-start service?* parameter is set to n. The default is 18 (yellow event indicator).
Event severity level for SNMP failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an SNMP failure has occurred. The default is 18 (yellow event indicator).
OID of any DHCP MIB counter	Provide the object identifier of any DHCP MIB counter you want checked. The default is .1.3.6.1.4.1.311.1.3.1.2.0.
Community	Specify the SNMP community string. The default is either the community string entered in AppManager Security Manager or *public* if no community string has been entered. The default is *public*.

DHCPLeases

Use this Knowledge Script to monitor the percentage of DHCP address leases that are being used. This script raises an event if the percentage of addresses used exceeds the threshold you set or the number of available addresses falls below the threshold you set. This script can monitor addresses for each DHCP scope individually or for the entire DHCP server.

The concept of a DHCP address lease is one in which a client computer does not retain a permanent DHCP address. With a DHCP lease, a client computer communicates with a DHCP server on reboot to begin or confirm the lease of an address.

Prerequisite

This script requires the Microsoft SNMP service to be running.

Resource Object

DHCP service object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for total address usage?	Set to **y** to raise events when the percentage of addresses used or the number of available addresses exceeds the threshold for the entire DHCP server. The default is y.
Event for scope address usage?	Set to **y** to raise events when the percentage of addresses used or the number of available addresses exceeds the appropriate threshold for any DHCP scope. The default is y.
Collect data for total address usage?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of addresses in use. The default is n.
Collect data for scope address usage?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of addresses in use in a DHCP scope. The default is n.
Maximum threshold for the percentage of total addresses in use	Specify the maximum percentage of addresses that can be in use at one time for the entire DHCP server (total addresses available) before an event is raised. The default is 95%.
Maximum threshold for percentage of addresses in use in a scope	Specify the maximum percentage of addresses that can be in use in a DHCP scope before an event is raised. The default is 80%. A DHCP scope is the range of IP addresses that the DHCP server can assign to clients that are on one subnet.
Minimum threshold for total number of addresses available	Specify the minimum number of addresses that must be available for the DHCP server to prevent an event from being raised. The default is 10.

Parameter	How to Set It
Minimum threshold for number of addresses available in a scope	Specify the minimum number of addresses that must be available in a DHCP scope to prevent an event from being raised. The default is 5.
Event severity level for total usage high or availability low	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of addresses in use exceeds the threshold or the number of available addresses falls below the threshold. The default is 10 (red event indicator).
Event severity level for scope usage high or availability low	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of addresses in use in a scope exceeds the threshold or the number of available addresses in a scope falls below the threshold. The default is 15 (yellow event indicator).
Community	Specify the SNMP community string. The default is either the community name entered in AppManager Security Manager or *public* if no community name has been entered. The default is *public*.

DNSHealthCheck

Use this Knowledge Script to monitor the availability, CPU usage, memory usage, and name resolution of the Domain Name System (DNS) service. By default, this script attempts to restart the DNS service if the service is not running.

Resource Object

DNS service object

Default Schedule

The default interval for this script is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event when DNS service is down?	Set to **y** to raise an event when the DNS service is down. The default is y.
Event when DNS name resolution fails?	Set to **y** to raise an event when name resolution fails. If set to y, the script attempts to resolve the specified hostname to the specified IP address. If the name resolution fails, an event is raised. If set to n, the script does not perform a name resolution lookup, and the *Hostname for name resolution* and *Host IP address that should be returned* parameters are ignored. The default is y.
Event when DNS CPU usage is over threshold?	Set to **y** to raise an event when the percentage of CPU consumed by the DNS service exceeds the threshold. The default is y.
Event when DNS memory usage is over threshold?	Set to **y** to raise an event when the amount of memory consumed by the DNS service exceeds the threshold. The default is y.
Collect data for DNS service up/down?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the DNS service is running, or • **0** -- the service is not running. The default is n.
Collect data for DNS CPU usage?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the percentage of CPU consumed by the DNS service. The default is n.
Collect data for DNS memory usage?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the amount of memory, in kilobytes (KB), consumed by the DNS service. The default is n.
Auto-start service?	Set to **y** to automatically restart the DNS service if it is down. The default is y.
Event severity level for service down; restart failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DNS service is down and the script cannot restart the service. The default is 5 (red event indicator).
Event severity level for service down; restart succeeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DNS service is down and the script successfully restarted the service. The default is 25 (blue event indicator).

Parameter	How to Set It
Event severity level for service down; don't restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DNS service is down and the *Auto-start service?* parameter is set to n. The default is 18 (yellow event indicator).
Event severity level for NS lookup failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DNS name resolution function fails. The default is 8 (red event indicator).
Event severity level for CPU usage exceeded threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 8 (red event indicator).
Event severity level for memory usage exceeded threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. The default is 8 (red event indicator).
Event severity level for external command failed to execute	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a system error prevents the execution of the DNS service. The default is 8 (red event indicator).
DNS process % CPU maximum threshold	Specify the maximum percentage of CPU resources that can be consumed by the DNS process before an event is raised. The default is 10%.
DNS process memory usage maximum threshold	Specify the maximum amount of memory resources that can be consumed by the DNS process before an event is raised. The default is 1024 KB.
Hostname for name resolution	Specify the name of the host to look up if you are using this script to test the hostname-to-IP address resolution. Default is localhost.
Host IP address that should be returned	Specify the correct IP address that should be returned by the DNS service if you are using this script to test the hostname-to-IP address resolution. The default is 127.0.0.1.

DNSSync

Use this Knowledge Script to check connectivity between two DNS servers. This script compares the DNS time stamp serial number for the current site with the time stamp serial number for the DNS site you specify. Both the remote site hostname and DNS domain name are required. This script raises an event if the serial numbers of the DNS servers are out of sync by more than the threshold value.

Resource Object

DNS service object

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the serial numbers of the DNS servers are out of sync by more than the threshold value. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the servers are in sync, or • **0** -- the servers are out of sync by more than the threshold value. In either case, the difference between the local and remote serial numbers is recorded in the detail message. The default is n.
DNS serial number difference maximum threshold	Specify the maximum difference that can occur between the local and remote DNS serial numbers before an event is raised. The default is 10.
Remote DNS host name	Specify the name of the DNS host computer. The default is `eclipse.netiq.com.`
DNS domain name	Specify the name of the DNS domain on the remote server. The default is netiq.com.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the serial numbers of the DNS servers are out of sync by more than the threshold value. The default is 8 (red event indicator).

RASConnections

Use this Knowledge Script to monitor the average number of connections to the Remote Access Server (RAS). This script raises an event if the total number of connections per minute exceeds the threshold you set.

Resource Object

RAS service object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the total number of connections to the RAS per minute exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the average number of connections to the RAS per minute during the monitoring interval. The default is n.
Connections per minute maximum threshold	Specify the maximum number of connections to the server that can occur per minute before an event is raised. The default is 50 connections per minute.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of connections per minute exceeds the threshold. The default is 8 (red event indicator).

RASErrors

Use this Knowledge Script to monitor the total number of Remote Access Server (RAS) errors in an interval. Remote access server errors can include CRC errors, alignment errors, and timeout errors, for example. This script raises an event if the total number of errors exceeds the threshold.

Resource Object

RAS service object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the total number of errors exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the difference between the number of RAS errors during the last monitoring interval and the number of RAS errors during the current monitoring interval. The default is n.
Total number of errors maximum threshold	Specify the maximum number of errors that can occur before an event is raised. The default is 50 errors.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of errors exceeds the threshold. The default is 8 (red event indicator).

RASHealthCheck

Use this Knowledge Script to check the availability of the Remote Access Server (RAS) service. This script raises an event if the RAS service is not running and attempts to restart the service if the service is not running.

Resource Object

RAS service object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event when RAS service is down?	Set to **y** to raise an event when the RAS service is down. The default is y.
Collect data for RAS service up/down?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the RAS service is running, or • **0** -- the RAS service is not running. The default is n.
Auto-start service?	Set to **y** to automatically restart down services. The default is y.
Check RasMan?	Set to **y** to check whether the Remote Access Connection Manager (`RasMan`) service is running. The default is n.
Event severity level for service down; restart failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the RAS service is down and this script could not restart the service. The default is 5 (red event indicator).
Event severity level for service down; restart succeeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the RAS service is down and this script successfully restarted the service. The default is 25 (blue event indicator).
Event severity level for service down; don't restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the RAS service is down and the *Auto-start service?* parameter is set to n. The default is 18 (yellow event indicator).

RASStat

Use this Knowledge Script to monitor the traffic on the Remote Access Server (RAS) server. This script raises an event if the total number of bytes transferred (transmitted and received) exceeds the threshold you set.

Resource Object

RAS service object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the total number of bytes transferred per second by the RAS server since the script was last run exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of bytes transferred by the RAS server since the script was last run. The default is n.
Total bytes per second maximum threshold	Specify the maximum total number of bytes that can be transferred per second before an event is raised. The default is 500 bytes per second.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the total number of transferred bytes exceeds the threshold. The default is 8 (red event indicator).

WINSConflict

Use this Knowledge Script to monitor conflict activity on the Windows Internet Name Service (WINS) server. This script raises an event if the number of group and unique conflicts per second exceeds the threshold you set.

Group conflicts per second is the rate at which group registrations received by the WINS server resulted in conflicts with records in the database. *Unique conflicts* per second is the rate at which unique registrations and renewals received by the WINS server resulted in conflicts with records in the database

Resource Object

WINS service object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event when the number of conflicts per second exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of unique conflicts and group conflicts per second. The default is n.
Total conflicts per second maximum threshold	Specify the maximum number of group and unique conflicts that can occur per second before an event is raised. The default is 4 conflicts per second.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of group and unique conflicts exceeds the threshold. The default is 8 (red event indicator).

WINSFailure

Use this Knowledge Script to report the number of failures per second on the Windows Internet Name Service (WINS) server. This script raises an event if the total failure rate for queries and releases exceeds the threshold you set.

Resource Object

WINS service object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the total failure rate for queries and releases on the WINS server exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of failed queries and failed releases per second. The default is n.
Total failures per second maximum threshold	Specify the maximum number of failures that can occur per second before an event is raised. The default is 2 failures per second.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of failures exceeds the threshold. The default is 8 (red event indicator).

WINSHealthCheck

Use this Knowledge Script to check the availability and CPU usage of the Windows Internet Name Service (WINS) service. This script raises an event if the WINS service is not running or if CPU usage exceeds the threshold you set. In addition, this script attempts to restart the WINS service if the service is not running.

Resource Object

WINS service object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event when WINS service is down?	Set to **y** to raise an event if the WINS service is not running. The default is y.
Event when WINS CPU usage is over threshold?	Set to **y** to raise an event if the percentage of CPU consumed by the WINS service exceeds the threshold. The default is y.
Collect data for WINS service up/down?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the WINS service is running, or • **0** -- the service is not running. The default is n.
Collect data for WINS CPU usage?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the percentage of CPU used by the WINS service. The default is n.
Auto-start service?	Set to **y** to automatically restart down services. The default is y.
Event severity level for service down; restart failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the WINS service is down and this script cannot restart it. The default is 5 (red event indicator).
Event severity level for service down; restart succeeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the WINS service is down and this script successfully restarted the service. The default is 25 (blue event indicator).
Event severity level for service down; don't restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the WINS service is down and the *Auto-start service?* parameter is set to n. The default is 18 (yellow event indicator).
Event severity level for CPU usage exceeded threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold you set. The default is 8 (red event indicator).
WINS process %CPU maximum threshold	Specify the maximum percentage of CPU that the WINS process can consume before an event is raised. The default is 60%.

WINSQueries

Use this Knowledge Script to monitor query activity on the Windows Internet Name Service (WINS) server. This script raises an event when query failure rate or the total number of queries exceeds the threshold you set.

Resource Object

WINS service object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event when the total number of queries per second or the number of failed queries per second exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of failed and successful queries per second. The default is n.
Failed query maximum threshold	Specify the maximum number of failed queries that can occur per second before an event is raised. The default is 2 query failures per second.
Total query maximum threshold	Specify the maximum number of queries that can occur per second before an event is raised. The default is 50 queries.
Event severity level for failed queries exceeded threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of failed queries exceeds the threshold you set. The default is 8 (red event indicator).
Event severity level for total queries exceeded threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the total number of queries exceeds the threshold you set. The default is 25 (blue event indicator).

WINSReplication

Use this Knowledge Script to monitor replication activity on the Windows Internet Name Service (WINS) server. This script raises an event if either a planned or network-triggered replication does not occur within the specified period.

Prerequisite

This script requires the Microsoft SNMP service to be running.

Resource Object

WINS service object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Community	Provide the SNMP community string. The default is either the community name entered in AppManager Security Manager or *public* if no community name has been entered.
Event if planned replication failed?	Set to **y** to raise events when planned replications fail. The default is y.
Event if network-triggered replication failed	Set to **y** to raise events when network-triggered replications fail. The default is y.
Number of minutes without planned replication maximum threshold	Specify the maximum number of minutes to wait for a planned replication. If replication does not occur within the elapsed time, this script assumes that the planned replication failed. The default is 60 minutes.
Number of minutes without network replication maximum threshold	Specify the maximum number of minutes to wait for a network-triggered replication. If replication does not occur within the elapsed time, this script assumes that the network replication failed. The default is 60 minutes.
Event severity level for planned replication failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a planned replication fails. The default is 8 (red event indicator).
Event severity level for network-triggered replication failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a network-triggered replication fails. The default is 15 (yellow event indicator).
Event severity level for SNMP failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an SNMP failure occurs. The default is 18 (yellow event indicator).

WINSStat

Use this Knowledge Script to monitor the total registrations, renewals, and releases on the Windows Internet Name Service (WINS) server. This script raises an event when the number of registrations, renewals, or releases per second exceeds the threshold you set.

Resource Object

WINS service object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events when the total number of registrations, renewals, or releases per second on the WINS server exceeds the thresholds you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total numbers of registrations, renewals, and releases per second on the WINS server. The default is n.
Registrations per second maximum threshold	Specify the maximum number of registration requests that can occur per second before an event is raised. The default is 20 requests per second.
Renewals per second maximum threshold	Specify the maximum number of renewal requests that can occur per second before an event is raised. The default is 20 requests per second.
Releases per second maximum threshold	Specify the maximum number of release requests that can occur per second before an event is raised. The default is 20 requests per second.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15 (yellow event indicator).

Chapter 46
NetworkDevice Knowledge Scripts

AppManager for Network Devices provides the following Knowledge Scripts for monitoring network devices such as routers, switches, and voice gateways by means of SNMP polling of Management Information Bases (MIBs). Using SNMP `GET` commands, NetworkDevice scripts monitor the basic subsystems that are common to all devices, such as CPU, memory, and the chassis.

AppManager for Network Devices supports SNMP versions 1, 2, and 3.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ATMLink_QoS	Monitors QoS on ATM links on a Cisco IOS device for traffic class usage, dropped packet rate, and queue depth.
ATMLink_Util	Monitors the usage of the parent resource of the ATM links on a network device.
Chassis_Usage	Monitors the physical chassis of a network device, including CPU, RAM, flash memory, backplane, temperature sensors, voltage sensors, and fan sensors.
Device_Ping	Checks the availability of network devices that respond to ICMP Echo requests.
Device_Syslog	Listens for UDP traffic on port 514.
Device_Uptime	Monitors the number of hours that a network device or its network management component has been operational since its last reboot.
FrameRelayLink_QoS	Monitors QoS on frame relay links on a Cisco IOS device for traffic class usage, dropped packet rate, and queue depth.
FrameRelayLink_Util	Monitors the usage of a parent resource for the frame relay links on a network device.
FXOPort_Health	Monitors signal errors on an FXO port on a network device.
FXOPort_Util	Monitors FXO port usage on a network device.
FXSPort_Health	Monitors signal errors on an FXS port on a network device.
FXSPort_Util	Monitors FXS port usage on a network device.
Host_CPULoaded	Accesses the Host Resource MIB to monitor CPU usage on a device.
Host_DeviceStatus	Accesses the Host Resource MIB to monitor the status and error count for a device.
Host_MemoryUsage	Accesses the Host Resource MIB to monitor memory usage on a device.

Knowledge Script	What It Does
Host_ProcessDown	Accesses the Host Resource MIB to determine whether a specified process is not running on a device.
Host_ProcessUp	Accesses the Host Resource MIB to determine whether a specified process is running on a device.
Host_StorageUsage	Accesses the Host Resource MIB to monitor storage usage on a device.
Interface_Health	Monitors the parent resource for the interfaces on a network device.
IPSubsystem_Util	Monitors the IP subsystem of a network device.
ISDNChannel_CallVolume	Measures the number of incoming calls, the number of outgoing calls, and the percentage of call failures (dropped calls) on a device.
ISDNChannel_Health	Monitors the operational status of ISDN bearer channels and the up-or-down status of signaling channels.
ISDNChannel_Util	Measures the usage of ISDN channels on a device.
LANLink_QoS	Monitors QoS on LAN links on a Cisco IOS device for traffic class usage, dropped packet rate, and queue depth.
LANLink_Util	Monitors the parent resource for the LAN links on a network device.
Report_ChassisUsage	Summarizes the Good-Acceptable-Poor (GAP) and average usage for CPU, memory pool, and backplane for a network device.
Report_DeviceAvailability	Summarizes the availability of selected network devices.
Report_ISDNCallVolume	Summarizes the average ISDN channel call volume for the links on selected devices.
Report_ISDNTimeDetail	Summarizes the average ISDN statistics on selected trunks.
Report_ISDNUtilization	Summarizes the average ISDN channel call volume for the trunks on selected devices.
Report_LinkUtilization	Summarizes average link usage.
Report_QoSUtilization	Summarizes average traffic class statistics for the links on selected devices.
Report_QoSVolume	Summarizes average traffic class statistics for the links on selected devices.
Report_TotalVolume	Summarizes total volume for selected devices.
SingleATMLink_Util	Monitors the usage of the ATM links on a single network device.
SingleFrameRelayLink_Util	Monitors the usage of frame relay links on a single network device.
SingleInterface_Health	Monitors the health of interfaces on a single network device.
SingleLANLink_Util	Monitors the usage of the LAN links on a single network device.
SingleWANLink_Util	Monitors the usage of the serial, T1, or T3 links on a single network device.
SNMPTrap_AddMIB	Add management information bases for monitoring by the SNMPTrap_Async Knowledge Script.
SNMPTrap_Async	Checks for incoming SNMP traps forwarded from NetIQ SNMP Trap Receiver.
WANLink_QoS	Monitors QoS on WAN links on a Cisco IOS device for traffic class usage, dropped packet rate, and queue depth.
WANLink_Util	Monitors the parent resource for the serial, T1, or T3 links on a network device.
Recommended Knowledge Scripts	Identifies the scripts recommended for optimal monitoring of network devices.

ATMLink_QoS

Use this Knowledge Script to monitor Quality of Service (QoS) on ATM links on a Cisco IOS device. This script monitors traffic class usage, dropped packet rate, and queue depth. In addition, this script raises an event if a monitored item exceeds the threshold that you set and generates datastreams for all monitored items.

Traffic class

A particular category of traffic on an interface. For example, voice and data can be classified as individual traffic classes.

Queue

The virtual buffer associated with a particular traffic class.

Dropped packet rate

The rate at which packets are dropped because of factors such as queuing, policing, early detection, or traffic shaping.

Queue depth

The number of packets in a queue.

Policy

The action that QoS takes within a traffic class upon the traffic that enters the class, such as dropping packets. Pre-policy traffic is the traffic that flows into a traffic class, before QoS applies a policy. Post-policy is the traffic that leaves a traffic class after a policy has been applied.

Resource Object

NetworkDevice ATM Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General	
Link name filter	Using regular expression, specify the names of the ATM links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** • To monitor all ATM links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude interface name filter.* • To monitor all ATM links, enter *"*"* and select **Include** in *Include or exclude link name filter.* • To monitor nothing, enter *"*"* and select **Exclude** in *Include or exclude link name filter.*

Parameter	How to Set It
Include or exclude link name filter	Select **Include** to monitor only the ATM links you specified in *Link name filter*. Select **Exclude** to monitor all ATM links except those you specified in *Link name filter.*
Class name filter	Using regular expression, specify the names of the traffic classes you want to monitor. Leave this parameter blank to monitor all traffic classes.
Traffic Class Utilization	
Monitor traffic class utilization?	Set to **y** to monitor traffic class usage and to activate the parameters in this section. The default is y.
Collect data for traffic class utilization?	Set to **y** to collect data for charts and graphs. The default is n. This script generates datastreams for the pre-policy and post-policy bandwidth used by each configured traffic class.
Threshold - Maximum traffic class utilization	Specify the highest percentage of traffic class usage that can occur before an event is raised. The default is 25%.
Event severity when traffic class utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of traffic class usage exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Collect data for traffic class pre/post policy bytes?	Set to **y** to collect data for charts and graphs. The default is n. This script creates datastreams for the number of pre- and post-policy bytes per second.
Queue Depth	
Monitor queue depth?	Set to **y** to monitor queue depth and to activate the parameters in this section. The default is y.
Collect data for queue depth?	Set to **y** to collect data for charts and graphs. The default is n. This script generates datastreams for queue depth (number of packets) by class name.
Threshold - Maximum priority queue depth	Specify the maximum number of packets that a priority queue can contain before an event is raised. The default is 0 packets.
Threshold - Maximum non-priority queue depth	Specify the highest number of packets that a non-priority queue can contain before an event is raised. The default is 10 packets.
Event severity when queue depth exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the queue depth exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Dropped Packets	
Monitor dropped packet rate?	Set to **y** to monitor the rate at which packets are dropped from the traffic class and to activate the parameters in this section. The default is y.
Collect data for dropped packet rate?	Set to **y** to collect data for charts and graphs. the default is n. This script generates datastreams for the percentage of dropped packets, and for the number of packets dropped per second.
Threshold - Maximum dropped packet rate	Specify the maximum rate at which packets can be dropped from the traffic class before an event is raised. The default is 1%.

Parameter	How to Set It
Event severity when dropped packet rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the dropped packet rate exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

ATMLink_Util

Use this Knowledge Script to monitor the usage of the parent resource of the Asynchronous Transfer Mode (ATM) links on a network device. This script raises an event if a monitored value exceeds the threshold that you set. In addition, this script generates datastreams for bandwidth usage, packet rate, and packet error rate.

Note
ATMLink_Util differs from SingleATMLink_Util in that it lets you monitor all links for all devices of any parent resource. SingleATMLink_Util allows you to monitor selected links for only one device.

You should understand your network's normal behavior so that you know when to examine usage levels more closely.

Determine usage levels on your current network: ethernet, Fiber Distributed Data Interface (FDDI), token ring, and Asynchronous Transfer Mode (ATM). On most networks, usage gradually increases as users begin using more network resources, such as email, network printing, and file sharing. Be concerned with usage peaks that *do not* follow this pattern.

Examine your network's typical usage over time and note whether your network has experienced a gradual or sudden increase in usage.

- A sharp increase in usage indicates an abnormal condition. Search the area of the network where the increase occurred. For example, a device may be causing "broadcast storms."
- A sustained high or low level of usage indicates an increasing or decreasing load on your network. If necessary, redistribute network traffic by segmenting your LAN with a bridge, router, or switch.

Resource Object

NetworkDevice ATM Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General	
Link name filter	Using regular expression, specify the names of the ATM links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** • To monitor all ATM links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* • To monitor all ATM links, enter *"*"* and select **Include** in *Include or exclude link name filter.* • To monitor nothing, enter *"*"* and select **Exclude** in *Include or exclude link name filter.*

Parameter	How to Set It
Include or exclude link name filter	Select **Include** to monitor only the ATM links you specified in *Link name filter*. Select **Exclude** to monitor all ATM links except those you specified in *Link name filter.*
Link Utilization	
Monitor link utilization?	Set to **y** to monitor link usage and to activate the parameters in this section. The default is y.
Collect data for bandwidth utilization?	Set to **y** to collect data about bandwidth usage for charts and graphs. The default is y.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Set to **y** to collect data about sent and received bytes for charts and graphs. The default is y.
Collect data for inbound/outbound bandwidth utilization?	Set to **y** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is n.
Link Errors	
Monitor link errors?	Set to **y** to monitor link errors and to activate the parameters in this section. The default is y.
Collect data for link errors?	Set to **y** to collect data about link errors for charts and graphs. The default is n.
Threshold - Maximum packet errors	Specify the maximum percentage of packet errors that can occur before an event is raised. The default is 50%.
Event severity when packet errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

Chassis_Usage

Use this Knowledge Script to monitor the physical chassis of a network device and create datastreams for the following:

- CPU usage
- Memory buffer error rate
- Backplane usage
- Voltage values
- Fan status
- Memory poll usage
- Flash memory usage
- Temperature values
- Power supply status

This script raises an event if any value exceeds a specified threshold. In addition, this script generates datastreams for CPU usage, RAM usage, flash memory usage, backplane usage, temperature and voltage states, and power supply and fan status.

Troubleshooting Events

The topic discusses possible causes and corrective actions for events that are raised when usage exceeds the threshold you set. You should understand your network's normal behavior so that you know when to examine usage levels more closely.

Determine usage levels on your current network: ethernet, Fiber Distributed Data Interface (FDDI), token ring, and Asynchronous Transfer Mode (ATM). On most networks, usage gradually increases as users begin using more network resources, such as email, network printing, and file sharing. Be concerned with usage peaks that *do not* follow this pattern.

Examine your network's typical usage over time and note whether your network has experienced a gradual or sudden increase in usage.

- A sharp increase in usage indicates an abnormal condition. Search the area of the network where the increase occurred. For example, a device may be causing "broadcast storms."
- A sustained high or low level of usage indicates an increasing or decreasing load on your network. If necessary, redistribute network traffic by segmenting your LAN with a bridge, router, or switch.

Resource Object

NetworkDevice Chassis Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
CPU	
Monitor CPU?	Set to **y** to monitor CPU usage and to activate the parameters in this section. The default is y.

Parameter	How to Set It
Collect data for CPU utilization?	Set to **y** to collect data about CPU usage for charts and reports. The default is y.
Threshold - Maximum CPU utilization	Specify the maximum percentage of CPU usage that can occur before an event is raised. The default is 50%.
Event severity when CPU utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which CPU usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive CPU usage. The default is 10.
RAM	
Monitor RAM?	Set to **y** to monitor RAM usage and to activate the parameters in this section. The default is y. RAM usage includes NVRAM, DRAM, and SRAM, depending on whether you are monitoring a switch or a router.
Collect data for RAM utilization?	Set to **y** to collect data about RAM usage for charts and reports. The default is y.
Threshold - Maximum memory pool utilization	Specify the maximum percentage of memory pool usage that can occur before an event is raised. The default is 50%.This figure represents the maximum usage for all memory pools (NVRAM, DRAM, and SRAM).
Event severity when memory pool utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which memory pool usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive memory pool usage. The default is 10.
Threshold - Maximum memory buffer error rate	Specify the maximum number of memory buffer errors that can occur per second before an event is raised. The default is 0.
Event severity when memory buffer error rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the number of memory buffer errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive memory buffer error rate. The default is 10.
Flash Memory	
Monitor flash memory?	Set to **y** to monitor flash memory and to activate the parameters in this section. The default is y.
Collect data for flash memory utilization?	Set to y to collect data about flash memory usage for charts and reports. The default is n.
Threshold - Maximum flash memory utilization	Specify the maximum percentage of flash memory usage that can occur before an event is raised. The default is 90%.
Event severity when flash memory utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which flash memory usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive flash memory usage. The default is 10.
Backplane	
Monitor backplane?	Set to **y** to monitor backplane usage and to activate the parameters in this section. The default is y.
Collect data for backplane utilization?	Set to **y** to collect data about backplane usage for charts and reports. The default is y.
Threshold - Maximum backplane utilization	Specify the maximum percentage of backplane usage that can occur before an event is raised. The default is 75%.

Parameter	How to Set It
Event severity when backplane utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which backplane usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive backplane usage. The default is 10.
Temperature Sensors	
Monitor temperature sensors?	Set to **y** to monitor temperature sensors and to activate the parameters in this section. The default is y.
Collect data for temperature?	Set to **y** to collect data about temperature states for charts and reports. The default is n.
Threshold - Maximum temperature	Specify the maximum temperature that can be reached before an event is raised. The default is 50 degrees Celsius.
Event severity when temperature exceeds threshold or sensor state not OK	Set the severity level, between 1 and 40, to indicate the importance of an event in which the temperature exceeds the threshold that you set or if the state of the temperature sensor is not "OK." Enter **0** if you do not want to raise an event. The default is 10.
Voltage Sensors	
Monitor voltage sensors?	Set to **y** to monitor voltage sensors and to activate the parameters in this section. The default is y.
Collect data for voltage sensor state?	Set to **y** to collect data about voltage states for charts and reports. The default is n.
Event severity when voltage state not OK	Set the severity level, between 1 and 40, to indicate the importance of an event in which the voltage state is not "OK." The default is 10.
Power Supplies	
Monitor power supplies?	Set to **y** to monitor power supplies and to activate the parameters in this section. The default is y.
Collect data for power supply state?	Set to **y** to collect data about power supply states for charts and reports. The default is n.
Event severity when power supply state not OK	Set the severity level, between 1 and 40, to indicate the importance of an event in which the power supply state is not "OK." The default is 10.
Fans	
Monitor fans?	Set to **y** to monitor fans and to activate the parameters in this section. The default is y.
Collect data for fan state?	Set to y to collect data about fan states for charts and reports. The default is n.
Event severity when fan state not OK	Set the severity level, between 1 and 40, to indicate the importance of an event in which the fan state is not "OK." The default is 10.
DSP Cards	
Monitor DSP cards?	Set to **y** to monitor DSP (Digital Signal Processing) cards and to activate the parameters in this section. The default is y. DSP cards provide transcoding functionality between the PSTN and IP network.
Collect data for DSP card utilization?	Set to **y** to collect data about DSP card resource usage and status. The default is n.
Maximum DSP card utilization	Specify the maximum percentage of DSP card usage that can occur before an event is raised. The default is 75%.

Parameter	How to Set It
Event severity when DSP card utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which DSP card usage exceeds the threshold that you set. The default is 10.
Event severity when DSP card state not OK	Set the severity level, between 1 and 40, to indicate the importance of an event in which the DSP card state is not "Normal." Events will be raised for the following states: **Warning**, **Critical**, **Fatal**, and **offLine**. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

Device_Ping

Use this Knowledge Script to check the availability of network devices that respond to Internet Control Message Protocol (ICMP) Echo requests. This script raises an event if any value exceeds a specified threshold. In addition, this script generates datastreams for device availability.

Resource Object

NetworkDevice

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Collect data for device availability?	Set to **y** to collect data about timeouts and echo requests for charts and graphs. The default is y.
Event severity when Ping test fails	Set the severity level, between 1 and 40, to indicate the importance of an event in which a Ping test fails. For example, a Ping test could fail because the command is not found or because a device's IP address is incorrect. The default is 5.
Number of seconds before timeout	Specify the maximum number of seconds to wait for a response before timing out. The default is 3 seconds.
Number of echo requests to send	Specify the number of times to send the Ping echo request before raising an event. The default is 3 requests.
Threshold - Maximum number of consecutive timeouts	Specify the maximum number of consecutive timeouts that you want to allow before raising an event. The default is 1 timeout.

Device_Syslog

Syslog is a notification system by which devices on a network, such as routers, switches, and even hosts, can send notifications and alerts to a central server. Syslog traffic is transported by UDP over port 514. Use this Knowledge Script to listen for UDP traffic on port 514.

When you change a parameter value in the script while the job is running, the job stops and immediately restarts. It is possible for the job to restart before Windows has a chance to free the port 514. Therefore, the script job will fail on restart because it cannot listen on the Syslog port. You should wait 5 seconds or so before restarting the job. Waiting gives Windows a chance to free the port for listening.

Because AppManager performs active SNMP polling as well as passive Syslog monitoring, you may receive event notifications from both sources. For example, SNMP polling alerts AppManager when an interface goes down and, as a result, you receive an AppManager event. In addition, you may receive a Syslog message that provides the same information.

Prerequisite

Before using the Device_Syslog Knowledge Script, configure your network devices to send Syslog messages to the proxy agent computer. Configuration procedures are device specific. Consult the documentation for your particular device. The following procedure is for Cisco devices.

To configure Cisco devices:

1. Telnet to the device you want to configure.
2. Type the requested password and press [`Enter`].
3. Type `enable` and press [`Enter`].
4. Type the requested password and press [`Enter`].
5. Type `config` and press [`Enter`].
6. Type `logging <host name or IP address of device that you want to configure>`.
7. Exit.

Resource Object

NetworkDevice

Because this script listens on port 514, run this script only once on a proxy agent computer.

Default Schedule

By default, this script runs on an asynchronous schedule in order to report events as they occur. Once you start the Knowledge Script, its job status is "Running" and will remain so until you stop the job.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Monitor Syslog messages from all devices?	Set to **y** to accept all Syslog messages from all devices, including messages from devices that are not in the TreeView pane. If a device *is* in the TreeView pane, events are raised against the device. If a device *is not* in the TreeView pane, events are raised against the proxy agent computer. Set to **n** to monitor Syslog messages only from those devices on which you run this script. The default is n.
Message text filter	Using regular expression, provide the text you want to find in the Syslog. Leave this parameter blank to find all text.
Event severity when error messages found	Set the severity level, between 1 and 40, to indicate the importance of an event in which error messages are found in the log. The default is 5. Set the severity level to **0** if you do not want to raise an event.
Event severity when warning messages found	Set the severity level, between 1 and 40, to indicate the importance of an event in which warning messages are found in the log. The default is 15. Set the severity level to **0** if you do not want to raise an event.
Event severity when informational messages found	Set the severity level, between 1 and 40, to indicate the importance of an event in which informational messages are found in the log. The default is 0. Set the severity level to **0** if you do not want to raise an event.

Device_Uptime

Use this Knowledge Script to monitor one of the following:

- The number of hours that a network device has been operational since it was last restarted.
- The number of hours that a device's network management component, such as the SNMP agent, has been operational since it was last restarted.

This script raises an event if the device is restarted during the monitoring interval. In addition, this script generates datastreams for device uptime.

In the event of a device restart, you can set an action on the Actions tab to automatically run the Action_RunDiscoveryNetworkDevice Knowledge Script. The Action script discovers network device resources on the rebooted device.

Resource Object

NetworkDevice

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Collect data for uptime?	Set to **y** to collect data about uptime for charts and graphs. The default is n. This script generates a datastream for the number of hours that a device has been operational since its last reboot or for the number of hours that the management component has been operational since its last restart. The datastream legend is the same for host or management component: "`Device uptime [<device>] (hours)`"
Monitor host uptime or uptime of the network management portion of the system	Select whether to monitor the device itself or the device's management component: • Select **Host uptime** to monitor the uptime of a host device. • Select **Management component uptime** to monitor the management component of a device, independent of the uptime of the host device.
Event severity when device reboots	Set the severity level, between 1 and 40, to indicate the importance of an event in which the monitored device has been rebooted. Set the severity level to **0** if you do not want to raise an event. The default severity level is 5.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

FrameRelayLink_QoS

Use this Knowledge Script to monitor Quality of Service (QoS) on frame relay links on a Cisco IOS device. This script monitors traffic class usage, dropped packet rate, and queue depth. This script raises an event if a monitored item exceeds the threshold that you set and generates datastreams for traffic class usage, dropped packet rates, and queue depth by class name.

Traffic class

A particular category of traffic on an interface. For example, voice and data can be classified as individual traffic classes.

Queue

The virtual buffer associated with a particular traffic class.

Dropped packet rate

The rate at which packets are dropped because of factors such as queuing, policing, early detection, or traffic shaping.

Queue depth

The number of packets in a queue.

Policy

The action that QoS takes within a traffic class upon the traffic that enters the class, such as dropping packets. Pre-policy traffic is the traffic that flows into a traffic class, before QoS applies a policy. Post-policy refers to the traffic that leaves a traffic class after a policy has been applied.

Resource Object

NetworkDevice FR Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General	
Link name filter	Using regular expression, specify the names of the frame relay links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** • To monitor all frame relay links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* • To monitor all frame relay links, enter `"*"` and select **Include** in *Include or exclude link name filter.* • To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter.* • To monitor only serial links, enter `(?=serial)` and select **Include** in *Include or exclude link name filter.* • To monitor all interfaces EXCEPT serial links, enter `(?=serial)` and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the frame relay links you specified in *Link name filter*. Select **Exclude** to monitor all frame relay links except those you specified in *Link name filter.*
Class name filter	Using regular expression, specify the name of the traffic classes that you want to monitor. Leave this parameter blank to monitor all traffic classes.
Traffic Class Utilization	
Monitor traffic class utilization?	Set to **y** to monitor traffic class usage and to activate the parameters in this section. The default is y.
Collect data for traffic class utilization?	Set to **y** to collect data for charts and graphs. The default is n. This script creates datastreams for the pre-policy and post-policy bandwidth used by each configured traffic class.
Threshold - Maximum traffic class utilization	Specify the maximum percentage of traffic class usage that can occur before an event is raised. The default is 25%.
Event severity when traffic class utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of traffic class usage exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Collect data for traffic class pre/post policy bytes?	Set to **y** to collect data for charts and graphs. The default is n. This script creates datastreams for the number of pre-policy and post-policy bytes per second.
Queue Depth	
Monitor queue depth?	Set to **y** to monitor queue depth and to activate the parameters in this section. The default is y.
Collect data for queue depth?	Set to **y** to collect data for charts and graphs. The default is n. This script generates datastreams for queue depth (number of packets) by class name.
Threshold - Maximum priority queue depth	Specify the maximum number of packets that a priority queue can contain before an event is raised. The default is 0 packets.

Parameter	How to Set It
Threshold - Maximum non-priority queue depth	Specify the highest number of packets that a non-priority queue can contain before an event is raised. The default is 10 packets.
Event severity when queue depth exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the queue depth exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Dropped Packets	
Monitor dropped packet rate?	Set to **y** to monitor the rate at which packets are dropped from the traffic class and to activate the parameters in this section. The default is y.
Collect data for dropped packet rate?	Set to **y** to collect data for charts and graphs. The default is n.This script generates datastreams for the percentage of dropped packets, and for the number of packets dropped per second.
Threshold - Maximum dropped packet rate	Specify the maximum rate at which packets can be dropped from the traffic class before an event is raised. The default is 1%.
Event severity when dropped packet rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the dropped packet rate exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

FrameRelayLink_Util

Use this Knowledge Script to monitor the usage of a parent resource for the frame relay links on a network device. A frame relay link uses a packet-switching protocol for connecting devices on a Wide Area Network (WAN). This script raises an event if a monitored value exceeds the threshold you set. In addition, this script generates datastreams for the following:

- Bandwidth usage
- Frame rate
- FECN (Forward Explicit Congestion Notification) rate. A *FECN* is a frame relay message that notifies the receiving device when there is congestion in the network. A FECN bit is sent in the direction in which the frame is traveling, toward its destination.
- BECN (Backward Explicit Congestion Notification) rate. A *BECN* is a frame relay message that notifies the sending device when there is congestion in the network. A BECN bit is sent in the direction from which the frame is traveling, toward its transmission source.

Note
FrameRelayLink_Util differs from SingleFrameRelayLink_Util in that it lets you monitor all links for all devices of any parent resource. SingleFrameRelayLink_Util allows you to monitor selected links for only one device.

Resource Object

NetworkDevice FR Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General	
Link name filter	Using regular expression, specify the names of the frame relay links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** • To monitor all frame relay links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* • To monitor all frame relay links, enter `"*"` and select **Include** in *Include or exclude link name filter.* • To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter.* • To monitor only serial links, enter `(?=serial)` and select **Include** in *Include or exclude link name filter.* • To monitor all interfaces EXCEPT serial links, enter `(?=serial)` and select **Exclude** in *Include or exclude link name filter.*

Parameter	How to Set It
Include or exclude link name filter	Select **Include** to monitor only the frame relay links you specified in *Link name filter*. Select **Exclude** to monitor all frame relay links except those you specified in *Link name filter.*
Link Utilization	
Monitor link utilization?	Set to **y** to monitor link usage and to activate the parameters in this section. The default is y.
Collect data for link bandwidth utilization?	Set to **y** to collect data about bandwidth usage for charts and graphs. The default is y.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Set to **y** to collect data about sent and received bytes for charts and graphs. The default is y.
Collect data for inbound/outbound bandwidth utilization?	Set to **y** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is n.
Link Errors	
Monitor FECNs/BECNs?	Set to **y** to monitor FECN and BECN rates and to activate the parameters in this section. The default is y.
Collect data for FECNs/BECNs?	Set to **y** to collect data about FECN and BECN rates for charts and graphs. The default is n.
Threshold - Maximum FECNs/BECNs	Specify the maximum percentage of FECN/BECN rates that can occur before an event is raised. The default is 8%.
Event severity when FECNs/BECNs exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of FECN/BECN rates exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

FXOPort_Health

Use this Knowledge Script to monitor signal errors on a Foreign Exchange Office (FXO) port on a network device. This script raises an event if the number of signal errors exceeds the specified threshold. In addition, this script generates datastreams for signal errors.

Resource Object

NetworkDevice FXO Port Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Collect data for signal errors?	Set to **y** to collect data about signal errors for charts and graphs. The default is n.
Threshold - Maximum signal errors	Specify the maximum number of signal errors that can occur before an event is raised. The default is 0 errors.
Event severity when signal errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the number of signal errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive signal errors. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

FXOPort_Util

Use this Knowledge Script to monitor Foreign Exchange Office (FXO) port usage on a network device. This script raises an event if port usage exceeds the specified threshold. In addition, this script generates datastreams for port usage.

Resource Object

NetworkDevice FXO Port Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Collect data for FXO port utilization?	Set to **y** to collect data about port usage for charts and graphs. The default is y.
Threshold - Maximum FXO port utilization	Specify the maximum percentage of port usage that can occur before an event is raised. The default is 80%.
Event severity when port utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which port usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event for port usage. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

FXSPort_Health

Use this Knowledge Script to monitor signal errors on a Foreign Exchange Station (FXS) port on a network device. This script raises an event if the number of signal errors exceeds the specified threshold. In addition, this script generates datastreams for signal errors.

Resource Object

NetworkDevice FXS Port Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Collect data for signal errors?	Set to **y** to collect data about signal errors for charts and graphs. The default is n.
Threshold - Maximum signal errors	Specify the maximum number of signal errors that can occur before an event is raised. The default is 0 errors.
Event severity when signal errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the number of signal errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive signal errors. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

FXSPort_Util

Use this Knowledge Script to monitor Foreign Exchange Station (FXS) port usage on a network device. This script raises an event if port usage exceeds the specified threshold. In addition, this script generates datastreams for port usage.

Resource Object

NetworkDevice FXS Port Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Collect data for FXS port utilization?	Set to **y** to collect data about port usage for charts and graphs. The default is y.
Threshold - Maximum FXS port utilization	Specify the maximum percentage of port usage that can occur before an event is raised. The default is 80%.
Event severity when port utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which port usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event for port usage. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

Host_CPULoaded

Use this Knowledge Script to access the Host Resource MIB to monitor CPU usage on a host device. This script raises an event if CPU usage exceeds the threshold that you set. In addition, this script generates a datastream for percentage of CPU usage during the monitoring period.

Note
For a Nortel CS1000 version 4.5 Call Server, this script monitors call capacity usage rather than CPU usage. In version 4.5 devices, the MIB value for the CPU processor load represents call capacity usage.

Resource Object

NetworkDevice Host Processor

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Collect data for CPU utilization?	Set to **y** to collect data for charts, graphs, and reports. When enabled, data collection returns the overall CPU usage percentage. The default is n.
Threshold - Maximum CPU utilization	Specify the maximum CPU usage that must occur before an event is raised. The default is 50%.
Event severity when CPU utilization exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. If you do not want to raise an event, set the severity level to **0**. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

Host_DeviceStatus

Use this Knowledge Script to access the Host Resource MIB to monitor the status of a device and the number of errors that have occurred since the last iteration of the script. This script raises an event if a device is down or if errors occur. In addition, this script generates datastreams for device status and the number of errors.

Note
This script retrieves the error count from the DeviceErrors field of the Host Resource MIB.

Resource Object

NetworkDevice Host Device

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Raise event if device is down?	Set to **y** to raise an event if the monitored device is down. The default is y.
Event severity when device is down	Set the severity level, between 1 and 40, to indicate the importance of an event in which the monitored device is down. The default is 10.
Collect data for device status?	Set to **y** to collect data for charts, graphs, and reports. When enabled, data collection returns 100 if the device is up or 0 if the device is down. The default is n.
Raise event if device errors occur?	Set to **y** to raise an event if errors occurred since the last iteration of the script. The default is y.
Event severity when device errors occur	Set the severity level, between 1 and 40, to indicate the importance of an event in which errors occurred since the last iteration of the script. The default is 10.
Collect data for device errors?	Set to **y** to collect data for charts, graphs, and reports. When enabled, data collection returns a datastream for the number of errors that have occurred since the last iteration of the script. The default is n.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

Host_MemoryUsage

Use this Knowledge Script to access the Host Resource MIB to monitor memory usage on a device. This script raises an event if memory usage exceeds the threshold you set. In addition, this script generates a datastream for memory usage on the device.

Resource Object

NetworkDevice Host Memory

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Collect data for memory usage?	Set to **y** to collect data for charts, graphs, and reports. When enabled, data collection returns the percentage of memory usage for the monitoring period. The default is n.
Threshold - Maximum memory usage	Specify the maximum memory usage that must occur before an event is raised. The default is 90%.
Event severity when memory usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. If you do not want to raise an event, set the severity level to **0**. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

Host_ProcessDown

Use this Knowledge Script to access the Host Resource MIB to determine whether specified processes are not running. This script raises an event if a specified process is not running. In addition, this script generates datastreams for process status.

Resource Object

NetworkDevice Host Processor Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Raise event if process is not running?	Set to **y** to raise an event if a specified process is not running. The default is y.
Collect data for process status?	Set to **y** to collect data for charts and reports. If enabled, data collection returns a value of 100 when a specified process is running, or a value of 0 when the process is not running. The default is n.
Processes to monitor	Specify one or more process names, separated by commas and no spaces. For example: `grep.exe,batch.exe` **Note** If the device being monitored is running on Microsoft Windows, the process name specified should match the Image Name seen on the Process tab in Task Manager.
Event severity when process is not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which specified processes are not running. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

Host_ProcessUp

Use this Knowledge Script to access the Host Resource MIB to verify whether a specified process is running. This script raises an event if a specified process is running and generates datastreams for process status.

Resource Object

NetworkDevice Host Processor Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Raise event if process is running?	Set to **y** to raise an event if a specified process is running. The default is y.
Collect data for process status?	Set to **y** to collect data for charts and reports. If enabled, data collection returns a value of 100 when a specified process is running, or a value of 0 when the process is not running. The default is n.
Processes to monitor	Specify one or more process names, separated by commas and no spaces. For example: `grep.exe,batch.exe` **Note** If the device being monitored is running on Microsoft Windows, the process name specified should match the Image Name seen on the **Process** tab in Task Manager.
Event severity when process is running	Set the severity level, from 1 to 40, to indicate the importance of an event in which the specified processes are running. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

Host_StorageUsage

Use this Knowledge Script to access the Host Resource MIB to monitor storage usage on a device. This script raises an event if storage usage exceeds the threshold that you set. In addition, this script generates a datastream for storage usage on the device.

Resource Object

NetworkDevice Host Storage

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Collect data for storage usage?	Set to **y** to collect data for charts, graphs, and reports. When enabled, data collection returns the percentage of storage usage for the monitoring period. The default is n.
Threshold - Maximum storage usage	Specify the maximum storage usage that can occur before an event is raised. The default is 90%.
Event severity when storage usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which storage usage exceeds the threshold. If you do not want to raise an event, set the severity level to **0**. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

Interface_Health

Use this Knowledge Script to monitor the parent resource for the interfaces on a network device. This script raises an event if the interface status changes or if any value exceeds a specified threshold. This script generates datastreams indicating the number of "up" interfaces and the total number of interfaces.

Note
Interface_Health differs from SingleInterface_Healthin that it lets you monitor all interfaces for all devices of any parent resource. SingleInterface_Health allows you to monitor selected interfaces for only one device.

Troubleshooting Events

The table below identifies possible causes and corrective actions for events that are raised when an interface's status changes. These events can lead to unacceptable service levels for an interface that remains down.

Narrow the usage problem to ports that have excessively high or low usage. If necessary, redistribute network traffic by segmenting your LAN with a bridge, router, or switch.

Determine usage levels on your current network. Try to locate the segments that are experiencing high or low usage levels, which are an indicator of the usage on the chassis.

Possible Cause	Corrective Action
No cable connected	Reconnect the cable on the switch to a known good device.
Wrong port	Ensure both ends of the cable are plugged into the correct ports.
Device has no power	Ensure both devices are powered on and connected to a power source.
Wrong cable type	Verify your cable selection.
Bad cable	Swap the suspect cable with a known good cable. Look for broken or missing pins on the connector.
Loose connections	Unplug a cable and reinsert it. A cable may not be as fully seated in a jack as it appears.
Patch panels	Eliminate faulty patch panel connections. If possible, bypass the patch panel to rule it out as a possible cause.
Media convertors	Eliminate faulty media convertors, such as fiber-to-copper. If possible, bypass the media convertor to rule it out as a possible cause.
Bad or wrong gigabit	Swap the suspect GBOC with a known good GBIC.
Interface convertor (GBIC)	Verify hardware and software support for this type of GBIC.
Bad port or module	Move the cable to a known good port to troubleshoot a suspect port or module.
Port, interface, or module not enabled	Use the `show port` command for CatOS or the `show interface` command for Cisco IOS to look for errdisable, disable, or shutdown status. Use the `show module` command to look for faulty status, which could indicate a hardware problem.

Resource Object

NetworkDevice Interface Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Filter details	
Interface name filter	Using regular expression, provide the name of the interface for the devices you want to monitor or the devices you do not want to monitor. **Examples** • To monitor all interfaces, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude interface name filter.* • To monitor all interfaces, enter `"*"` and select **Include** in *Include or exclude interface name filter.* • To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude interface name filter.* • To monitor only ethernet interfaces, enter `(?=Ethernet)` and select **Include** in *Include or exclude interface name filter.* • To monitor all interfaces EXCEPT ethernet interfaces, enter `(?=Ethernet)` and select **Exclude** in *Include or exclude interface name filter.*
Include or exclude interface name filter	Select **Include** to monitor only the devices for the interfaces you specified in *Interface name filter*. Select **Exclude** to monitor all devices except for those associated with the interfaces you specified in *Interface name filter.*
Collect data for operational interfaces and total interfaces?	Set to **y** to collect data about the number of interfaces that are operational and the total number of interfaces for use in charts and reports. The default is n.
Event severity when interface goes down	Set the severity level, between 1 and 40, to indicate the importance of an event in which the interface's operational status changes from Up to Down. Enter **0** if you do not want to raise an event. The default is 5. By default, this script raises one event only when the operational status changes to Down. If you want to raise an event every time the Knowledge Script runs to indicate that the interface is *still* down, use the *Raise the "Interface down" event on every job iteration* parameter.
Event severity when interface comes up	Set the severity level, between 1 and 40, to indicate the importance of an event in which the interface's operational status changes from Down to Up. Enter **0** if you do not want to raise an event. The default is 25.
Event severity when interface goes administratively down	Set the severity level, between 1 and 40, to indicate the importance of an event in which the interface's administrative status changes from Up to Down. The default is 15. By default, this script raises one event only when the administrative status changes to Down. If you want to raise an event every time the Knowledge Script runs to indicate that the interface is *still* down, use the *Raise the "Interface down" event on every job iteration* parameter.
Event severity when interface comes administratively and operationally back up	Set the severity level, between 1 and 40, to indicate the importance of an event in which the interface's administrative *and* operational statuses change from Down to Up. The default is 30.

Parameter	How to Set It
Raise the “Interface down” event on every job iteration	Set to **y** to raise an event for each job iteration in which an interface’s operational or administrative status is Down. To raise one event only when the status changes from Up to Down, set this parameter to n. The default is n.
Ignore the administratively down interfaces	Set to **y** to prevent AppManager from raising an event when an interface is down for administrative purposes. Accept the default of **n** if you want AppManager to raise an event when an interface is down for administrative purposes.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

IPSubsystem_Util

Use this Knowledge Script to monitor the IP subsystem of a network device, including inbound and outbound packet rates and packet error rates. This script raises an event if the packet error rate exceeds the threshold you set. In addition, this script generates datastreams for packet error rates and the number of packet errors.

Resource Object

NetworkDevice IP Subsystem

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Collect data for packet rate and packet errors?	Set to **y** to collect data about packet rates and packet errors for charts and graphs. The default is n.
Threshold - Maximum packet error rate	Specify the maximum packet error rate that can occur before an event is raised. The default is 8%.
Event severity when packet error rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the packet error rate exceeds the threshold that you set. Enter **0** if you do not want to raise an event for excessive packet error rate. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

ISDNChannel_CallVolume

Use this Knowledge Script to measure the number of incoming calls, the number of outgoing calls, and the percentage of call failures (dropped calls) on a device. This script raises an event if the dropped call rate exceeds the threshold you set. In addition, this script generates datastreams for incoming and outgoing call rates and dropped calls.

Resource Object

NetworkDevice ISDN Channel Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Filter Details	
Channel name filter	Using regular expression, specify the names of the channels you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude channel name filter* parameter. **Examples** • To monitor all channels, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude channel name filter.* • To monitor all channels, enter **"*"** and select **Include** in *Include or exclude channel name filter.* • To monitor nothing, enter **"*"** and select **Exclude** in *Include or exclude channel name filter.*
Include or exclude channel name filter	Select **Include** to monitor only the channels you specified in *Channel name filter*. Select **Exclude** to monitor all channels except those you specified in *Channel name filter.*
Collect data for call rate and dropped calls?	Set to **y** to collect data about incoming call rates, outgoing call rates, and percentage of dropped calls for charts and graphs.
Threshold - Maximum dropped call rate	Specify the maximum percentage of dropped (failed) calls that can occur before an event is raised.
Event severity when dropped call rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of dropped calls exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

ISDNChannel_Health

Use this Knowledge Script to monitor the operational status of ISDN bearer channels and the up-or-down status of signaling channels. This script raises an event if the percentage of operational ISDN bearer channels falls below the threshold that you set or if a signaling channel is down. In addition, this script generates datastreams for operational ISDN bearer channels (as a percentage of all bearer channels) and signaling channel status.

Resource Object

NetworkDevice ISDN Channel Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Filter Details	
Channel name filter	Using regular expression, specify the names of the channels you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude channel name filter* parameter. **Examples** • To monitor all channels, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude channel name filter.* • To monitor all channels, enter **"*"** and select **Include** in *Include or exclude channel name filter.* • To monitor nothing, enter **"*"** and select **Exclude** in *Include or exclude channel name filter.*
Include or exclude channel name filter	Select **Include** to monitor only the channels you specified in *Channel name filter*. Select **Exclude** to monitor all channels except those you specified in *Channel name filter.*
Collect data for operational bearer channels?	Set to **y** to collect data for charts and graphs. If enabled, data collection returns the percentage of bearer channels that were operational during the monitoring period. The default is y.
Threshold - Minimum operational bearer channels	Specify the minimum percentage of channels that must be operational to prevent an event from being raised. The default is 99%.
Event severity when operational bearer channels fall below threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the number of operational channels falls below the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Collect data for ISDN signaling channel status?	Set to **y** to collect data for charts and graphs. If enabled, data collection returns 100 if the signaling channel is up and 0 if the signaling channel is down. The default is y.

Parameter	How to Set It
Event severity when the ISDN signaling channel is down	Set the severity level, between 1 and 40, to indicate the importance of an event in which the signaling channel is down. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

ISDNChannel_Util

Use this Knowledge Script to measure the usage of ISDN channels on a device. This script raises an event if channel usage exceeds the specified threshold. In addition, this script generates datastreams for ISDN channel usage.

Resource Object

NetworkDevice ISDN Channel Folder

Default Schedule

By default, this script runs every minute.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Filter Details	
Channel name filter	Using regular expression, specify the names of the channels you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude channel name filter* parameter. **Examples** • To monitor all channels, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude channel name filter.* • To monitor all channels, enter **"*"** and select **Include** in *Include or exclude channel name filter.* • To monitor nothing, enter **"*"** and select **Exclude** in *Include or exclude channel name filter.*
Include or exclude channel name filter	Select **Include** to monitor only the channels you specified in *Channel name filter*. Select **Exclude** to monitor all channels except those you specified in *Channel name filter.*
Collect data for ISDN channel utilization?	Set to **y** to collect data about channel usage for charts and graphs. The default is y.
Threshold - Maximum ISDN channel utilization	Specify the maximum percentage of channel usage that can occur before an event is raised. The default is 80%.
Event severity when ISDN channel utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of channel usage exceeds the threshold that you set. The default is 10. Set the severity level to **0** if you do not want to raise an event.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

LANLink_QoS

Use this Knowledge Script to monitor Quality of Service (QoS) on LAN links on a Cisco IOS device. This script monitors traffic class usage, dropped packet rate, and queue depth. This script raises an event if a monitored value exceeds the threshold you set.

Traffic class

A particular category of traffic on an interface. For example, voice and data can be classified as individual traffic classes.

Queue

The virtual buffer associated with a particular traffic class.

Dropped packet rate

The rate at which packets are dropped because of factors such as queuing, policing, early detection, or traffic shaping.

Queue depth

The number of packets in a queue.

Policy

The action that QoS takes within a traffic class upon the traffic that enters the class, such as dropping packets. Pre-policy traffic is the traffic that flows into a traffic class, before QoS applies a policy. Post-policy is the traffic that leaves a traffic class after a policy has been applied.

Resource Object

NetworkDevice LAN Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General	
Link name filter	Using regular expression, specify the names of the LAN links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** • To monitor all LAN links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* • To monitor all LAN links, enter `"*"` and select **Include** in *Include or exclude link name filter.* • To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter.* • To monitor only ip links, enter `(?=ip)` and select **Include** in *Include or exclude link name filter.* • To monitor all interfaces EXCEPT ip links, enter `(?=ip)` and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the LAN links you specified in *Link name filter*. Select **Exclude** to monitor all LAN links except those you specified in *Link name filter.*
Class name filter	Using regular expression, specify the name of the traffic classes that you want to monitor. Leave this parameter blank to monitor all traffic classes.
Traffic Class Utilization	
Monitor traffic class utilization?	Set to **y** to monitor traffic class usage and to activate the parameters in this section. The default is y.
Collect data for traffic class utilization?	Set to **y** to collect data for charts and graphs. This script generates datastreams for the pre-policy and post-policy bandwidth used by each configured traffic class. The default is n.
Threshold - Maximum traffic class utilization	Specify the maximum percentage of traffic class usage that can occur before an event is raised. The default is 25%.
Event severity when traffic class utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of traffic class usage exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Collect data for traffic class pre/post policy bytes?	Set to **y** to collect data for charts and graphs. The default is n. This script generates datastreams for the number of pre- and post-policy bytes per second.
Queue Depth	
Monitor queue depth?	Set to **y** to monitor the queue depth. The default is y.
Collect data for queue depth?	Set to **y** to collect data for charts and graphs. The default is n. This script generates datastreams for queue depth (number of packets) by class name.
Threshold - Maximum priority queue depth	Specify the highest number of packets that a priority queue can contain before an event is raised. The default is 0 packets.

Parameter	How to Set It
Threshold - Maximum non-priority queue depth	Specify the highest number of packets that a non-priority queue can contain before an event is raised. The default is 10 packets.
Event severity when queue depth exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the queue depth exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Dropped Packets	
Monitor dropped packet rate?	Set to **y** to monitor the rate at which packets are dropped from the traffic class and to activate the parameters in this section. The default is y.
Collect data for dropped packet rate?	Set to **y** to collect data for charts and graphs. The default is n. This script generates datastreams for the percentage of dropped packets, and for the number of packets dropped per second.
Threshold - Maximum dropped packet rate	Specify the maximum rate at which packets can be dropped from the traffic class before an event is raised. The default is 1%.
Event severity when dropped packet rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the dropped packet rate exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

LANLink_Util

Use this Knowledge Script to monitor the parent resource for the Local Area Network (LAN) links on a network device. This script creates datastreams for bandwidth usage, inbound and outbound packet rates, and inbound and outbound packet error rates. This script raises an event if a monitored value exceeds the threshold you set. In addition, this script generates datastreams for bandwidth usage and link errors.

Note
LANLink_Util differs from SingleLANLink_Util in that it lets you monitor all links for all devices of any parent resource. SingleLANLink_Util allows you to monitor selected links for only one device.

Resource Object

NetworkDevice LAN Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General	
Link name filter	Using regular expressions, specify the names of the LAN links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** • To monitor all LAN links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* • To monitor all LAN links, enter `"*"` and select **Include** in *Include or exclude link name filter.* • To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter.* • To monitor only ip links, enter `(?=ip)` and select **Include** in *Include or exclude link name filter.* • To monitor all interfaces EXCEPT ip links, enter `(?=ip)` and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the LAN links you specified in *Link name filter.* Select **Exclude** to monitor all LAN links except those you specified in *Link name filter.*
Link Utilization	
Monitor link utilization?	Set to **y** to monitor link usage and to activate the parameters in this section. The default is y.
Collect data for bandwidth utilization?	Set to **y** to collect data about bandwidth usage for charts and graphs. The default is 10.

Parameter	How to Set It
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Set to **y** to collect data about sent and received bytes for charts and graphs. The default is n.
Collect data for inbound/outbound bandwidth utilization?	Set to **y** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is n.
Link Errors	
Monitor link errors?	Set to **y** to monitor link errors and to activate the parameters in this section. The default is y.
Collect data for link errors?	Set to y to collect data about link errors for charts and graphs. The default is n.
Threshold - Maximum packet errors	Specify the maximum percentage of packet errors that can occur before an event is raised. The default is 8%.
Event severity when packet errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Include discards in link errors?	Set to **y** to include discarded incoming packets in the packet error calculation. The default is y. If set to y, the calculation for packet errors is as follows: `(notdeliveredpackets/deliveredpackets)*100%/ time elapsed` where *delivered packets* = sum(UCastPkts, NUCastPkts) and *not delivered packets* = sum(errors, discards, unknown protocols) Errors are defined as packet errors. Unknown protocols are unsupported protocols. Discards are packets discarded for any other reason.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

Report_ChassisUsage

Use this Knowledge Script to summarize the Good-Acceptable-Poor (GAP) ratings and average usage for CPU, memory pool, and backplane for a network device. This script uses the data collected by the Chassis_Usage Knowledge Script.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select device(s) for report	Select the network devices whose data you want to include in your report.
Select Knowledge Scripts	Select the Knowledge Scripts to include in your report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekdays	Select the days of the week to include in your report. The default is every day of the week.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Chart Thresholds	
Good-Acceptable CPU utilization threshold	Specify the Good-Acceptable CPU usage threshold to display on the charts in the report. The default is 30%.
Acceptable-Poor CPU utilization threshold	Specify the Acceptable-Poor CPU usage threshold to display on the charts in the report. The default is 50%.
Good-Acceptable memory pool utilization threshold	Specify the Good-Acceptable memory pool usage threshold to display on the charts in the report. The default is 30%.
Acceptable-Poor memory pool utilization threshold	Specify the Acceptable-Poor memory pool usage threshold to display on the charts in the report. The default is 50%.
Good-Acceptable backplane utilization threshold	Specify the Good-Acceptable backplane usage threshold to display on the charts in the report. The default is 50%.
Acceptable-Poor backplane utilization threshold	Specify the Acceptable-Poor backplane usage threshold to display on the charts in the report. The default is 75%.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Set to **y** to include charts of datastream values in the report. The default is y.

Parameter	How to Set It
Include tables?	Set to **y** to include tables of datastream values in the report. The default is y.
Select Average Utilization chart properties	Set chart properties, such as style, thresholds, and size. The default style is Area.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceChassisUsage.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device Chassis Usage Summary.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_DeviceAvailability

Use this Knowledge Script to summarize the availability of selected network devices over a specified time period. This script uses the data collected by the Device_Ping Knowledge Script.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select devices for report	Select the network devices whose data you want to include in your report.
Select Knowledge Script	Specify the name of the Knowledge Script to include in your report. Specify one script per report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Report Settings	
Decimal accuracy for % values	Specify the number of decimal places that you want to see in the percentage values generated by this report. The default is 3.
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Set to **y** to include charts of datastream values in the report. The default is y.
Include tables?	Set to **y** to include a table of datastream values in the report. The default is y.
Select chart style	Define the graphic properties of the charts in your report. The default chart style is Line.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceAvailability.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID helps you correlate a specific instance of a Report script with the corresponding report.

Parameter	How to Set It
Select properties	Set the report properties as desired. The default report name is Network Device Availability.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_ISDNCallVolume

Use this Knowledge Script to summarize the average ISDN channel call volume for the links on selected devices over a time range. This Knowledge Script uses data collected by the ISDNChannel_CallVolume Knowledge Script.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select device(s) for report	Select the network devices whose data you want to include in your report.
Select granularity filter	Select **Trunk** or **Gateway** to determine the granularity of data gathered for your report. Selecting **Trunk** generates one chart per gateway, while selecting **Gateway** generates a single chart displaying data for each gateway. The default is Trunk.
Select Knowledge Scripts	Select the Knowledge Scripts to include in your report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Chart Thresholds	
Call volume threshold	Specify the call volume threshold to display on the charts in the report. Accept the default of **0** if you do not want to display this threshold.
Dropped call threshold	Specify the dropped call threshold to display on the charts in the report. Accept the default of **0** if you do not want to display this threshold.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Set to **y** to include charts of datastream values in the report. The default is y.
Include tables?	Set to **y** to include tables of datastream values in the report. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceISDNChannelCallVolume.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID helps you correlate a specific instance of a Report script with the corresponding report.

Parameter	How to Set It
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device ISDN Channel Call Volume Summary.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_ISDNTimeDetail

Use this Knowledge Script to summarize the average ISDN statistics on selected trunks over a time range. This script uses data collected by the ISDNChannel_Util and ISDNChannel_CallVolume Knowledge Scripts.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select link(s) for report	Select the links whose data you want to include in your report.
Select Knowledge Scripts	Select the Knowledge Scripts to include in your report.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Set to **y** to include charts of datastream values in the report. The default is y.
Include tables?	Set to **y** to include tables of datastream values in the report. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceISDNTimeDetail.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device ISDN Time Detail Summary.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event Notification	

Parameter	How to Set It
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_ISDNUtilization

Use this Knowledge Script to summarize the average ISDN channel call volume for the trunks on selected devices over a time range. This script uses the data collected by the ISDNChannel_CallVolume Knowledge Script.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select device(s) for report	Select the network devices whose data you want to include in your report.
Select granularity filter	Select **Trunk** or **Gateway** to determine the granularity of data gathered for your report. Selecting **Trunk** generates one chart per gateway, while selecting **Gateway** generates a single chart displaying data for each gateway. The default is Trunk.
Select Knowledge Scripts	Select the Knowledge Scripts to include in your report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Chart Thresholds	
Good-Acceptable channel utilization threshold	Specify the Good-Acceptable channel usage threshold to display on the charts in the report. The default is 30%.
Acceptable-Poor channel utilization threshold	Specify the Acceptable-Poor channel usage threshold to display on the charts in the report. The default is 50%.
Channel utilization threshold	Specify the channel usage threshold to display on the charts in the report. Accept the default of 0% if you do not want to display this threshold.
Channel Utilization Chart Settings	
Select chart properties	Set chart properties, such as style, thresholds, and size. The default chart style is Bar.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Set to **y** to include charts of datastream values in the report. The default is y.
Include tables?	Set to **y** to include a table of datastream values in the report. The default is y.

Parameter	How to Set It
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceISDNChannelUtilization.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device ISDN Channel Utilization Summary.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_LinkUtilization

Use this Knowledge Script to summarize average link usage within a specified time frame. This script uses the data collected by the link usage Knowledge Scripts.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select device(s) for report	Select the network devices whose data you want to include in your report.
Select Knowledge Script	Select the Knowledge Script to include in your report. Select one script per report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Chart Thresholds	
Good-Acceptable bandwidth utilization threshold	Specify the Good-Acceptable bandwidth usage threshold to display on the charts in the report. The default is 30%.
Acceptable-Poor bandwidth utilization threshold	Specify the Acceptable-Poor bandwidth usage threshold to display on the charts in the report. The default is 50%.
Total volume threshold	Specify the volume threshold to display on the charts in the report. Enter **0** if you do not want to display a threshold. The default is 0 bytes/second.
Packet Errors Chart Settings	
Select chart properties	Set chart properties, such as style, thresholds, and size. The default chart style is Bar.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Set to **y** to include charts of datastream values in the report. The default is y.
Include tables?	Set to **y** to include tables of datastream values in the report. The default is y.

Parameter	How to Set It
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceLinkUtilization.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device Link Utilization.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_QoSUtilization

Use this Knowledge Script to summarize average traffic class statistics for the links on selected devices over a time range. This script uses data collected by the link QoS Knowledge Scripts.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select device(s) for report	Select the network devices whose data you want to include in your report.
Select datastream type	Select the type of datastream to include in your report. The default is Post-policy bandwidth.
Select Knowledge Script	Specify the name of the Knowledge Script to include in your report. Specify one script per report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Set to **y** to include charts of datastream values in the report. The default is y.
Include tables?	Set to **y** to include tables of datastream values in the report. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceQoSUtilization.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device QoS Utilization Summary.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.

Parameter	How to Set It
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_QoSVolume

Use this Knowledge Script to summarize average traffic class statistics for the links on selected devices over a time range. This Knowledge Script uses data collected by the link QoS Knowledge Scripts.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select link(s) for report	Select the network devices whose data you want to include in your report.
Select datastream type	Select the type of datastream to include in your report. The default is Post-policy bandwidth.
Select Knowledge Script	Specify the name of the Knowledge Script to include in your report. Specify one Knowledge Script per report.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Set to **y** to include charts of datastream values in the report. The default is y.
Include tables?	Set to **y** to include tables of datastream values in the report. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceQoSVolume.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device QoS Volume Summary.

Parameter	How to Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_TotalVolume

Use this Knowledge Script to summarize total volume for selected devices within a specified time frame. This Knowledge Script uses the data collected by the link usage Knowledge Scripts.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Data Source	
Select device(s) for report	Select the network devices whose data you want to include in your report.
Select Knowledge Script	Provide the name of the Knowledge Script to include in your report. Specify one script per report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregate by	Select the time period by which the data in your report is aggregated. The default is Hour.
Chart Settings	
Chart size	Select the size of the rendered chart. Choose from **Large**, **Medium**, and **Small**. The default is Medium.
Horizontal chart?	Set to **y** to include a horizontal chart in your report. The default is n.
Chart color scheme	Select a color scheme template. The default template is NetIQ1.
Chart threshold value	Specify the threshold to be shown on reports. The default is 0 bytes/sec.
Report Settings	
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Set to **y** to include charts of datastream values in the report. The default is y.
Include tables?	Set to **y** to include tables of datastream values in the report. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is NetworkDeviceTotalVolume.

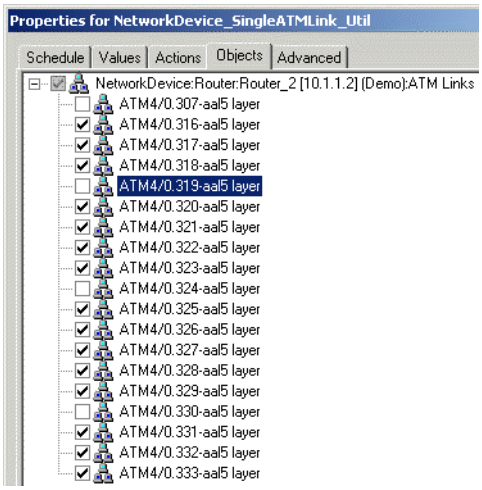
Parameter	How to Set It
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default report name is Network Device Total Volume.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event Notification	
Raise event when report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

SingleATMLink_Util

Use this Knowledge Script to monitor the usage of the Asynchronous Transfer Mode (ATM) links on a single network device. This script raises an event if any value exceeds a specified threshold. In addition, this script generates datastreams for bandwidth usage, packet rate, and packet error rate.

Note

SingleATMLink_Util differs from ATMLink_Util in that it allows you to choose the link you want to monitor for a single device. Click the Objects tab and select the appropriate links.



Resource Object

NetworkDevice

If you run the script on a large number of objects (roughly 100 or more), the Operator Console or Control Center console may take up to 30 seconds to display the Properties dialog box for the Knowledge Script. In addition, 100% of system CPU may be consumed during this 30-second period.

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Link Utilization	
Monitor link utilization?	Set to **y** to monitor link usage and to activate the parameters in this section. The default is y.
Collect data for bandwidth utilization?	Set to **y** to collect data about bandwidth usage for charts and graphs. The default is y.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.

Description	How to Set It
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Set to **y** to collect data about sent and received bytes for charts and graphs. The default is y.
Collect data for inbound/outbound bandwidth utilization?	Set to **y** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is n.
Link Errors	
Monitor link errors?	Set to **y** to monitor link errors and to activate the parameters in this section. The default is y.
Collect data for link errors?	Set to **y** to collect data about link errors for charts and graphs. The default is y.
Threshold - Maximum packet errors	Specify the maximum percentage of packet errors that can occur before an event is raised. The default is 8%.
Event severity when packet errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

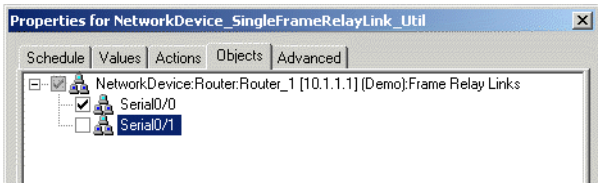
SingleFrameRelayLink_Util

Use this Knowledge Script to monitor the usage of the frame relay links on a single network device. A frame relay link uses a packet-switching protocol for connecting devices on a Wide Area Network (WAN). This script raises an event if any value exceeds a specified threshold. In addition, this script generates datastreams for the following:

- Bandwidth usage
- Frame rate
- FECN (Forward Explicit Congestion Notification) rate. A *FECN* is a frame relay message that notifies the receiving device that there is congestion in the network. A FECN bit is sent in the direction in which the frame is traveling, toward its destination.
- BECN (Backward Explicit Congestion Notification) rate. A *BECN* is a frame relay message that notifies the sending device that there is congestion in the network. A BECN bit is sent in the direction from which the frame is traveling, toward its transmission source.

Note

SingleFrameRelayLink_Util differs from FrameRelayLink_Util in that it allows you to choose which links you want to monitor for a single device. On the Objects tab, select the appropriate links. For example:



Resource Object

NetworkDevice

If you run the script on a large number of objects (roughly 100 or more), the Operator Console may take up to 30 seconds to display the Properties dialog box. In addition, 100% of system CPU may be consumed during this 30-second period.

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Link Utilization	
Monitor link utilization?	Set to **y** to monitor link usage and to activate the parameters in this section. The default is y.
Collect data for bandwidth utilization?	Set to **y** to collect data about bandwidth usage for charts and graphs. The default is y.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.

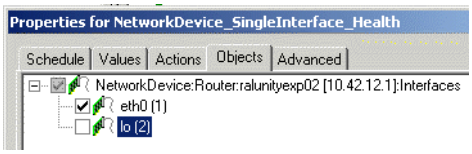
Parameter	How to Set It
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Set to **y** to collect data about sent and received bytes for charts and graphs. The default is y.
Collect data for inbound/outbound bandwidth utilization?	Set to **y** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is n.
Link Errors	
Monitor FECNs/BECNs?	Set to **y** to monitor FECN and BECN rates and to activate the parameters in this section. The default is y.
Collect data for FECNs/BECNs?	Set to **y** to collect data about FECN and BECN rates for charts and graphs. The default is y.
Threshold - Maximum FECNs/BECNs	Specify the maximum percentage of FECN/BECN rates that can occur before an event is raised. The default is 8%.
Event severity when FECNs/BECNs exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of FECN/BECN rates exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

SingleInterface_Health

Use this Knowledge Script to monitor the interfaces on a single network device. This script raises an event if the interface status changes or if any value exceeds a specified threshold. In addition, this script generates a datastream indicating the up or down status of the interface.

Note

SingleInterface_Health differs from Interface_Health in that it allows you to choose which interface you want to monitor for a single device. On the Objects tab, select the appropriate interfaces. For example:



Resource Object

NetworkDevice

If you run the script on a large number of objects (roughly 100 or more), the Operator Console or Control Center console may take up to 30 seconds to display the Properties dialog box for the Knowledge Script. In addition, 100% of system CPU may be consumed during this 30-second period.

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

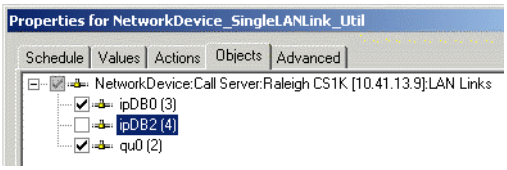
Parameter	How to Set It
Collect data for interface status?	Set to **y** to collect data about interface status for charts and graphs. The default is y.
Event severity when interface goes down	Set the severity level, between 1 and 40, to indicate the importance of an event in which the interface status changes from Up to Down. Enter **0** if you do not want to raise an event. The default is 5.
Event severity when interface comes back up	Set the severity level, between 1 and 40, to indicate the importance of an event in which the interface status changes from Down to Up. Enter **0** if you do not want to raise an event. The default is 15.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

SingleLANLink_Util

Use this Knowledge Script to monitor the Local Area Network (LAN) links on a single network device. This script raises an event if a threshold is exceeded. In addition, this script generates datastreams for bandwidth usage, inbound and outbound packet rates, and inbound and outbound packet error rates.

Note

SingleLANLink_Util differs from LANLink_Util in that it allows you to choose which links you want to monitor for a single device. On the Objects tab, select the appropriate links. For example:



Resource Object

NetworkDevice

If you run the script on a large number of objects (roughly 100 or more), the Operator Console or Control Center console may take up to 30 seconds to display the Properties dialog box for the Knowledge Script. In addition, 100% of system CPU may be consumed during this 30-second period.

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Link Utilization	
Monitor link utilization?	Set to **y** to monitor link usage and to activate the parameters in this section. The default is y.
Collect data for bandwidth utilization?	Set to **y** to collect data about bandwidth usage for charts and graphs. the default is y.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Set to **y** to collect data about sent and received bytes for charts and graphs. The default is y.
Collect data for inbound/outbound bandwidth utilization?	Set to **y** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is n.
Link Errors	

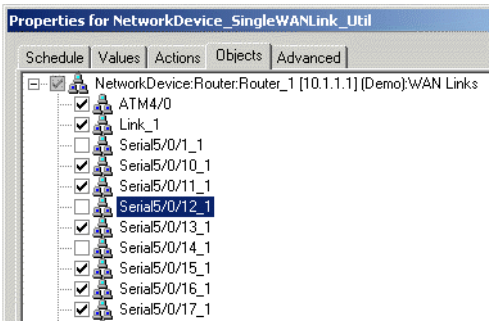
Parameter	How to Set It
Monitor link errors?	Set to **y** to monitor link errors and to activate the parameters in this section. The default is y.
Collect data for link errors?	Set to **y** to collect data about link errors for charts and graphs. The default is y.
Threshold - Maximum packet errors	Specify the maximum percentage of packet errors that can occur before an event is raised. The default is 8%.
Event severity when packet errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Include discards in link errors?	Set to **y** to include discarded incoming packets in the packet error calculation. The default is y. If set to y, the packet error calculation is as follows: `(notdeliveredpackets/deliveredpackets)*100%/ time elapsed` where *delivered packets* = sum(UCastPkts, NUCastPkts) and *not delivered packets* = sum(errors, discards, unknown protocols) Errors are defined as packet errors. Unknown protocols are unsupported protocols. Discards are packets discarded for any other reason.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

SingleWANLink_Util

Use this Knowledge Script to monitor the serial, T1, or T3 links on a single network device. This script raises an event if any value exceeds a threshold you set. In addition, this script generates datastreams for bandwidth usage, inbound and outbound packet rates, and inbound and outbound packet error rates.

Note

SingleWANLink_Util differs from WANLink_Util in that it allows you to choose the link you want to monitor for a single device. On the Objects tab, select the appropriate links. For example:



Resource Object

NetworkDevice

If you run the script on a large number of objects (roughly 100 or more), the Operator Console or Control Center console may take up to 30 seconds to display the Properties dialog box for the Knowledge Script. In addition, 100% of system CPU may be consumed during this 30-second period.

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Link Utilization	
Monitor link utilization?	Set to **y** to monitor link usage and to activate the parameters in this section. The default is y.
Collect data for bandwidth utilization?	Set to **y** to collect data about bandwidth usage for charts and graphs. The default is y.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Set to **y** to collect data about sent and received bytes for charts and graphs. The default is y.

Parameter	How to Set It
Collect data for inbound/outbound bandwidth utilization?	Set to **y** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is n.
Link Errors	
Monitor link errors?	Set to **y** to monitor link errors and to activate the parameters in this section. The default is y.
Collect data for link errors?	Set to **y** to collect data about link errors for charts and graphs. The default is y.
Threshold - Maximum packet errors	Specify the maximum percentage of packet errors that can occur before an event is raised. The default is 8%.
Event severity when packet errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Include discards in link errors?	Set to **y** to include discarded incoming packets in the packet error calculation. The default is y. If set to y, the calculation for packet errors is as follows: `(notdeliveredpackets/deliveredpackets)*100%/time elapsed` where *delivered packets* = sum(UCastPkts, NUCastPkts) and *not delivered packets* = sum(errors, discards, unknown protocols) Errors are defined as packet errors. Unknown protocols are unsupported protocols. Discards are packets discarded for any other reason.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

SNMPTrap_AddMIB

Use this Knowledge Script to add MIB (management information base) files to the MIB tree that is monitored by the SNMPTrap_Async Knowledge Script. The MIB files should be `ASN.1` text file with a `.txt` or `.my` file extension, and not compiled MIB files.

With this script you can copy a MIB file from an arbitrary directory to the MIB tree located in the `<AppManager directory>\bin\MIBs` directory. And, by using the *Reload MIB tree?* parameter, you can also reload all MIBs in the tree without restarting the AppManager agent. A restart of the AppManager agent automatically reloads the MIB tree.

Scenarios for using this script include the following examples:

In This Scenario	Set These Parameters
You want to add a MIB file to the MIB tree, but do not want the addition to take effect until after the next restart of the AppManager agent.	*Full path to MIB files* and *List of MIB files*: Provide location and name of MIB file you want to add. *Reload MIB tree?*: Set to **No** (unselected).
You manually copied a MIB file to the MIB directory and want to reload all MIBs in the directory.	*Full path to MIB files* and *List of MIB files*: Leave blank. *Reload MIB tree?*: Select **Yes**. *MIB reload timeout*: Set new timeout value or accept default of 10 seconds.
Due to compiler errors, you edited some MIBs in the MIB directory. Now you want to reload the MIBs to ensure the errors have been fixed.	*Full path to MIB files* and *List of MIB files*: Leave blank. *Reload MIB tree?*: Select **Yes**. *MIB reload timeout*: Set new timeout value or accept default of 10 seconds.

Resource Object

NetworkDevice Trap Receiver

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Full path to MIB files	Specify the full path to the folder that contains the MIB files you want to install. The AppManager agent on the proxy agent computer must have network access to the location you specify.
List of MIB files	Provide a comma-separated list of the MIB files you want to install. The MIB files should be `ASN.1` text files with a `.txt` or `.my` file extension. The MIB files should not be compiled MIB files. The MIB files you specify must be located in the folder you identified in the *Full path to MIB files* parameter.
Reload MIB tree?	Select **Yes** to update the MIB tree.

Parameter	How to Set It
MIB reload timeout	Specify the length of time AppManager should attempt to update the MIB tree before timing out and raising a failure event. The default is 10 seconds.
Event Notification	
Raise event if installation and reloading of MIB tree succeeds?	Select **Yes** to raise an event if installation of the MIB files and/or reloading of the MIB tree succeeds. The default is Yes. Note that reloading of the MIB tree can be successful even if no new MIB files are installed. Reloading of the MIB tree can proceed even if you provide no MIB files in the *List of MIB files* or *Full path to list of MIB files* parameter.
Event severity when installation and reloading of MIB tree succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the installation of MIB files and/or the reloading of the MIB tree succeeds. The default is 25.
Raise event if "reload MIB parser" warnings received?	Select **Yes** to raise an event if warning messages are received during the reload process. The default is Yes. Warning scenarios include: • MIBs are installed successfully but the *Reload MIB tree?* parameter is not set to Yes. • Not all specified MIB files were loaded to the MIB tree.
Event severity when "reload MIB parser" warnings received	Set the severity level, from 1 to 40, to indicate the importance of an event in which warning messages are received during the reload process. The default is 15.
Raise event if installation and reloading of MIB tree fails?	Select **Yes** to raise an event if AppManager fails to install or reload the specified MIB files. The default is Yes. Failure scenarios include: • MIB reload timeout period expired. • Not all specified MIB files were installed.
Event severity when installation and reloading of MIB tree fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the installation or reloading of the MIB tree fails. The default is 10.
Raise event with the list of currently installed MIBs?	Select **Yes** to raise an informational event that provides a list of all MIBs installed in the MIB tree. The default is Yes.
Event severity for list of currently installed MIBs	Set the severity level, from 1 to 40, to indicate the importance of an event that provides a list of all MIBs installed in the MIB tree. The default is 25.

SNMPTrap_Async

Use this Knowledge Script to check for SNMP traps forwarded from NetIQ SNMP Trap Receiver. This script raises an event when an SNMP trap is received and when Trap Receiver is unavailable or subsequently becomes available. In addition, this script generates datastreams for Trap Receiver availability.

This script checks for SNMP traps in the MIB tree. You can add Management Information Bases (MIBs) to the MIB tree. For more information, see the SNMPTrap_AddMIB Knowledge Script.

In general, a trap receiver is an application that receives traps from SNMP agents. NetIQ SNMP Trap Receiver (Trap Receiver) receives SNMP traps, filters them, and then forwards the traps to AppManager. For more information, see "Working with NetIQ SNMP Trap Receiver" on page 2586.

Resource Object

NetworkDevice Trap Receiver

Default Schedule

By default, this script runs on an asynchronous schedule.

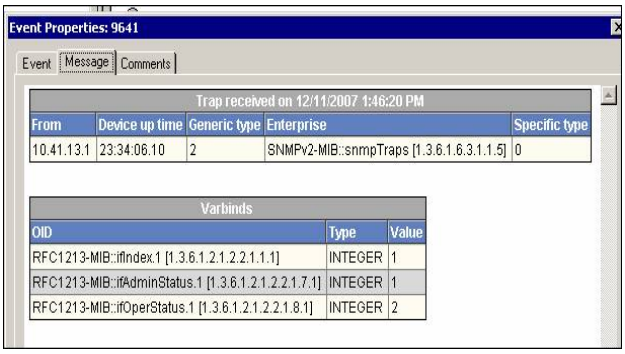
Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Trap Filters	
List of trap OIDs	Specify the OIDs (object identifiers) of the traps you want to monitor. You can type one OID or a list of OIDs. If you type a list, separate the OIDs with a comma. For example: `1.3.6.1.2.1.2.2.1.1.1,1.3.6.1.2.1.2.2.1.7.1`

Full path to file with list of trap OIDs	If you have many OIDs to monitor, you can provide the full path to a file that contains a list of the OIDs. Each OID in the file should be on a separate line. For example:
	`1.3.6.1.2.1.2.2.1.1.1`
	`1.3.6.1.2.1.2.2.1.7.1`
	Because the file must be accessible from the AppManager agent, the path must be a local directory on the agent computer or a UNC path.
	Important For a UNC path, the `netiqmc` service must have permission to access the path.

Event Notification	
Raise trap events?	Select **Yes** to raise an event when a trap message is received from Trap Receiver. The default is Yes.
Event severity when trap is received	Set the severity level, from 1 and 40, to indicate the importance of an event in which a trap is received. The default is 15.

Parameter	How to Set It
Format trap data according to SNMP version	Select the version of SNMP whose formatting should be used for trap event messages. The data provided by each format is the same; only the layout is different. An event message in SNMP v1 format looks like this:  An event message in SMMP v2 format looks like this: 
Raise Trap Receiver availability events?	Select **Yes** to raise an event when Trap Receiver becomes unavailable and when Trap Receiver becomes available once again. The default is Yes.
Event severity when Trap Receiver is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes unavailable. The default is 5.
Event severity when Trap Receiver becomes available	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes available after being unavailable. The default is 25.
Data Collection	
Collect data for Trap Receiver availability?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns a “1” if Trap Receiver is available and a “0” if Trap Receiver is unavailable. The default is unselected.
Interval for collecting Trap Receiver availability data	Specify the frequency with which the script collects Trap Receiver availability data. The default is every 5 minutes.

Working with NetIQ SNMP Trap Receiver

Installation of the AppManager for Network Devices module automatically installs Trap Receiver, which runs as a service: `NetIQTrapReceiver.exe`. Trap Receiver may compete for port usage with any other trap receiver installed on the same computer.

What is NetIQ SNMP Trap Receiver?

At its most basic, a trap receiver is an application that receives traps from SNMP agents. NetIQ SNMP Trap Receiver (Trap Receiver) receives, filters, and forwards SNMP traps to AppManager. When you use Trap Receiver with AppManager for Network Device, the SNMPTrap_Async Knowledge Script raises events when SNMP traps are received.

What is an SNMP Trap?

Simple Network Management Protocol (SNMP) is a protocol-based system used to manage devices on TCP/IP-based networks. From devices on which an SNMP agent resides, such as routers and switches, SNMP sends unsolicited notifications, called traps, to network administrators when thresholds for certain conditions are exceeded. These conditions are defined by the vendor in a device's Management Information Base (MIB); the network administrator sets the thresholds.

Traps are composed of Protocol Data Units (PDUs). Each PDU contains the following information, organized in various ways depending on the version of SNMP in use:

- SNMP version number
- Community name of the SNMP agent
- PDU type
- Enterprise OID (object identifier), a unique number that identifies an enterprise and its system objects in the MIB
- IP address of the SNMP agent
- Generic trap type: Cold start, Warm start, Link down, Link up, Authentication failure, and Enterprise
- Specific trap type. When the Generic trap type is set to "Enterprise," a specific trap type is included in the PDU. A specific trap is unique or specific to an enterprise.
- Time the event occurred
- Varbind (variable binding), a sequence of two fields that contain the OID and a value

Understanding Trap Receiver Architecture

Trap Receiver operates on a Client-Server architecture: the *Server*—the stand-alone Trap Receiver application—receives, filters, and forwards SNMP traps to the *Client*—an application that receives traps, such as AppManager. The Server may receive traps from standard UDP port 162 or from any other configured port. The Client and the Server can reside on the same computer or on separate (proxy) computers.

Communication between Client and Server is implemented as XML messages over a TCP connection. Only one Server is allowed per computer, however, several Clients are allowed per computer. Clients that are registered to the same Server share the same TCP connection. The Server TCP port should be known to all potential Clients.

Understanding the Trap Receiver Configuration File

The configuration file for Trap Receiver, `NetIQTrapReceiver.conf`, identifies the UDP and TCP ports used by Trap Receiver: the UDP port is used for receiving traps; the TCP port is used for communicating with the Client, such as AppManager or another supported NetIQ application. The configuration file also identifies the level of logging you want to use and whether port forwarding is enabled.

By default, the configuration file is installed in `[installation directory]\config`, and has the following format:

```
#################################################################
#
# NetIQTrapReceiver.conf
#
# A configuration file for NetIQ SNMP Trap Receiver
#
#################################################################

#########################
# TCP port
# Syntax: tcp_port [port]
# E.g. : tcp_port 2735
#########################
tcp_port 2735

#########################
# UDP port
# Syntax: udp_port [port]
# E.g. : udp_port 162
#########################
udp_port 162

#########################
# Forwarding
# Syntax: forward [address]:[port] [v1]
# E.g. : forward 127.0.0.1:1000 v1
#########################

#########################
# Log level
# Syntax: log_level error|warning|info|debug|xml
# E.g. : log_level info
#########################
log_level debug
```

If the configuration file cannot be found, cannot be parsed, or does not contain one of the required values, Trap Receiver is initialized with the default configuration as shown above.

When changing values in the configuration file, take into account the following:

- If you change the TCP port number, stop all asynchronous Knowledge Script jobs associated with the modules that support Trap Receiver. Run the Discovery Knowledge Script on all monitored devices to enable the devices to recognize the new TCP port number.
- If you change the UDP port number, also change the UDP port number configured on the devices that send traps to Trap Receiver.
- If another service uses port 2735 or port 162, Trap Receiver *will not start*. The Trap Receiver log file will contain different levels of messages, based on the log_level you choose. Either change the port numbers in the configuration file, stop the service that is using the default Trap Receiver port numbers, or forward the traps coming in to UDP port 162.
- To forward incoming traps to another trap receiver, such as Microsoft SNMP Trap Service, set the Forwarding values as follows:
  `forward [`*`IP address of other trap receiver`*`]:[`*`port number of other trap receiver`*`] [`*`SNMP version`*`]`.
  For example: `forward 10.40.40.25:167 v1`. By default, incoming traps are not forwarded. For more information, see "Coexisting with Microsoft SNMP Trap Service" on page 2589.
- Restart Trap Receiver after any change to the configuration file. From Control Panel, double-click **Administrative Tools** and then double-click **Services**. Right-click **NetIQ Trap Receiver** and select **Restart**.

Coexisting with Microsoft SNMP Trap Service

Two trap receivers cannot be in use on the same computer while using the same standard UDP port (162). If NetIQ SNMP Trap Receiver and another trap receiver such as Microsoft SNMP Trap Service are installed on the same computer and both are receiving traps, then configure Trap Receiver to use the standard UDP port and to forward incoming traps (UDP forwarding) to the other trap receiver. For more information, see "Understanding the Trap Receiver Configuration File" on page 2587.

Then, configure the other trap receiver to use a different, non-standard, UDP port that is not in use by another application. The following are instructions for configuring Microsoft SNMP Trap Service.

To configure Microsoft SNMP Trap Service to use another port:

1. Navigate to `c:\Windows\system32\drivers\etc`.
2. Open the **services** file.
3. In the row for `snmptrap`, change the value for **udp** from 162 to another port number that is not in use by any other application. Use the same port number you set as the forwarding port in the Trap Receiver configuration file.
4. Save and close the **services** file.
5. Restart Windows SNMP Trap Service. In Control Panel, double-click **Administrative Tools** and then double-click **Services**. Right-click **SNMP Trap Service** and select **Restart**.

Tip

To see which ports are in use, run `netstat.exe` from a command prompt. Then select an available port as the port for the other trap receiver service.

WANLink_QoS

Use this Knowledge Script to monitor Quality of Service (QoS) on WAN links on a Cisco IOS device. This script monitors traffic class usage, dropped packet rate, and queue depth. This script raises an event if a monitored value exceeds the threshold you set.

Traffic class

A particular category of traffic on an interface. For example, voice and data can be classified as individual traffic classes.

Queue

The virtual buffer associated with a particular traffic class.

Dropped packet rate

The rate at which packets are dropped because of factors such as queuing, policing, early detection, or traffic shaping.

Queue depth

The number of packets in a queue.

Policy

The action that QoS takes within a traffic class upon the traffic that enters the class, such as dropping packets. Pre-policy traffic is the traffic that flows into a traffic class, before QoS applies a policy. Post-policy is the traffic that leaves a traffic class after a policy has been applied.

Resource Object

NetworkDevice

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General	
Link name filter	Using regular expression, specify the names of the WAN links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** • To monitor all WAN links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* • To monitor all WAN links, enter `"*"` and select **Include** in *Include or exclude link name filter.* • To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter* • To monitor only serial links, enter `(?=serial)` and select **Include** in *Include or exclude link name filter.* • To monitor all interfaces EXCEPT serial links, enter `(?=serial)` and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the WAN links you specified in *Link name filter*. Select **Exclude** to monitor all WAN links except those you specified in *Link name filter.*
Class name filter	Using regular expression, specify the name of the traffic classes that you want to monitor. Leave this parameter blank to monitor all traffic classes.
Traffic Class Utilization	
Monitor traffic class utilization?	Set to **y** to monitor traffic class usage and to activate the parameters in this section. The default is y.
Collect data for traffic class utilization?	Set to **y** to collect data for charts and graphs. The default is n. This script generates datastreams for the pre-policy and post-policy bandwidth used by each configured traffic class.
Threshold - Maximum traffic class utilization	Specify the maximum percentage of traffic class usage that can occur before an event is raised. The default is 25%.
Event severity when traffic class utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of traffic class usage exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Collect data for traffic class pre/post policy bytes?	Set to **y** to collect data for charts and graphs. This script generates datastreams for the number of pre- and post-policy bytes per second. The default is n.
Queue Depth	
Monitor queue depth?	Set to **y** to monitor the queue depth. The default is y.
Collect data for queue depth?	Set to **y** to collect data for charts and graphs. The default is n. This script generates datastreams for queue depth (number of packets) by class name.
Threshold - Maximum priority queue depth	Specify the maximum number of packets that a priority queue can contain before an event is raised. The default is 0 packets.

Parameter	How to Set It
Threshold - Maximum non-priority queue depth	Specify the maximum number of packets that a non-priority queue can contain before an event is raised. The default is 10 packets.
Event severity when queue depth exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the queue depth exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Dropped Packets	
Monitor dropped packet rate?	Set to **y** to monitor the rate at which packets are dropped from the traffic class. The default is y.
Collect data for dropped packet rate?	Set to **y** to collect data for charts and graphs. The default is n. This script generates datastreams for the percentage of dropped packets, and for the number of packets dropped per second.
Threshold - Maximum dropped packet rate	Specify the maximum rate at which packets can be dropped from the traffic class before an event is raised. The default is 1%.
Event severity when dropped packet rate exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the dropped packet rate exceeds the threshold that you set. Set the severity level to **0** if you do not want to raise an event. The default is 10.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

WANLink_Util

Use this Knowledge Script to monitor the parent resource for the serial, T1, or T3 links on a network device. This script raises an event if a monitored value exceeds the threshold you set. In addition, this script generates datastreams for bandwidth usage, inbound and outbound packet rates, and inbound and outbound packet error rates.

Note
WANLink_Util differs from SingleWANLink_Utilin that it lets you monitor all links for all devices of any parent resource. SingleWANLink_Util allows you to monitor selected links for only one device.

Resource Object

NetworkDevice WAN Link Folder

Default Schedule

By default, this script runs every 5 minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
General	
Link name filter	Using regular expression, specify the names of the WAN links you want to monitor or do not want to monitor. Use this parameter in conjunction with the *Include or exclude link name filter* parameter. **Examples** • To monitor all WAN links, leave this parameter blank and select **Include** or **Exclude** in *Include or exclude link name filter.* • To monitor all WAN links, enter `"*"` and select **Include** in *Include or exclude link name filter.* • To monitor nothing, enter `"*"` and select **Exclude** in *Include or exclude link name filter* • To monitor only serial links, enter `(?=serial)` and select **Include** in *Include or exclude link name filter.* • To monitor all interfaces EXCEPT serial links, enter `(?=serial)` and select **Exclude** in *Include or exclude link name filter.*
Include or exclude link name filter	Select **Include** to monitor only the WAN links you specified in *Link name filter.* Select **Exclude** to monitor all WAN links except those you specified in *Link name filter.*
Link Utilization	

Parameter	How to Set It
Monitor link utilization?	Set to **y** to monitor link usage and to activate the parameters in this section. The default is y. **Hint** If you set this parameter to **n**, the WANLink_Util job does not raise events for usage and does not generate datastreams. To generate datastreams for usage without raising events, perform the following steps: 1. Set the *Monitor link utilization?* parameter to **y**. 2. Set the *Threshold - Maximum bandwidth utilization* parameter to 100%.
Collect data for bandwidth utilization?	Set to **y** to collect data about bandwidth usage for charts and graphs. The default is y.
Threshold - Maximum bandwidth utilization	Specify the maximum percentage of bandwidth usage that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the bandwidth usage exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Collect data for bytes sent/received?	Set to **y** to collect data about sent and received bytes for charts and graphs. The default is y.
Collect data for inbound/outbound bandwidth utilization?	Set to **y** to collect data for inbound/outbound bandwidth utilization. The data value is the maximum of the bandwidth inbound value or the bandwidth outbound value, whichever value is larger. The default is n.
Link Errors	
Monitor link errors?	Set to **y** to monitor link errors and to activate the parameters in this section. The default is y.
Collect data for link errors?	Set to **y** to collect data about link errors for charts and graphs. The default is n.
Threshold - Maximum packet errors	Specify the maximum percentage of packet errors that can occur before an event is raised. The default is 8%.
Event severity when packet errors exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold that you set. Enter **0** if you do not want to raise an event. The default is 10.
Include discards in link errors?	Set to **y** to include discarded incoming packets in the packet error calculation. The default is y. If set to y, the packet error calculation is as follows: `(notdeliveredpackets/deliveredpackets)*100%/time elapsed` where *delivered packets* = sum(UCastPkts, NUCastPkts) and *not delivered packets* = sum(errors, discards, unknown protocols) Errors are defined as packet errors. Unknown protocols are unsupported protocols. Discards are packets discarded for any other reason.
Raise one-time events?	Set to **y** to raise an event for all one-time events. For example, if you set this parameter to y, then, on the first iteration of this script, AppManager raises an event when a particular performance counter cannot be found. If you do not want to see such one-time events, set this parameter to **n**.

Recommended Knowledge Scripts

NetIQ Corporation recommends using the following Knowledge Scripts to ensure optimal monitoring of network devices.

- ATMLink_Util
- Chassis_Usage
- Device_Ping
- Device_Uptime
- FrameRelayLink_Util
- FXOPort_Health
- FXOPort_Util
- FXSPort_Health
- FXSPort_Util
- Interface_Health
- IPSubsystem_Util
- LANLink_Util
- WANLink_Util

Chapter 47
Networks-RT Knowledge Scripts

The Networks-RT category provides the following Knowledge Scripts and reports for monitoring network response time or throughput. Because these scripts simulate actual network transactions, you can use them to test the health and performance of your network.

From the Knowledge Script view of the Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
[ResponseTime]	Checks network response time.
[Throughput]	Tests network throughput.
Action_Traceroute	Collects exception traceroute data between a specified source and target location in response to an event in a separate Knowledge Script.
Action_TracerouteNetworks-RT	Collects exception traceroute data between a specified source and target location in response to an event in a separate Networks-RT Knowledge Script.
ActiveDirectoryAddUser	Emulates adding a user to a domain in the Active Directory.
ActiveDirectoryLogin	Emulates logging in to Active Directory.
ActiveDirectoryReplication	Emulates network traffic generated between two PCs during full domain directory replication.
ActiveDirectoryResetPassword	Emulates resetting a user's password in the Active Directory.
BaanAddItem	Emulates adding an item to a Baan database.
BaanGenerateMPSMRPBatches	Emulates generating MPS MRP batches in Baan.
BaanLoadDEM	Emulates loading Baan Dynamic Enterprise Management (DEM).
BaanLoadItemMaster	Emulates loading Baan Item Master.
BaanMaintainCustomer	Emulates performing Baan customer maintenance.
BaanMaintainEmployeeAdd	Emulates adding an employee to the Baan system.
BaanMaintainProductBom	Emulates maintenance of a standard Baan Bill of Materials (BOM).
BaanMaintainPurchaseOrder	Emulates maintaining a purchase order in the Baan system.
BaanMaintainSalesOrder	Emulates maintaining a sales order in the Baan system.
BaanMaintainServiceOrder	Emulates maintaining a service order in the Baan system.

Knowledge Script	What It Does
BaanPrintCompaniesListSelect	Emulates printing a list of selected companies in the Baan system.
BackWebSignupAndInfoPakDnld	Emulates subscribing to and downloading the contents of a new Back Web channel.
BackWebUpdate	Emulates updating an existing Back Web channel.
CastanetChannelDownload	Emulates downloading of Castanet channels.
CastanetInitialRun	Emulates a user running the Castanet Tuner for the first time.
ccMail	Emulates sending a mail message using ccMail.
CitrixICAExcelStartup	Emulates starting Excel within a Citrix Independent Computing Architecture (ICA)
CitrixICAIEStartup	Emulates starting Internet Explorer within a Citrix Independent Computing Architecture (ICA)
CitrixICAOutlookOpenFullBox	Emulates opening Outlook within a Citrix Independent Computing Architecture (ICA).
CitrixICATerminalServerLogon	Emulates logging on to a terminal server within a Citrix Independent Computing Architecture (ICA).
CitrixICAWordStartUp	Emulates starting MS Word within a Citrix Independent Computing Architecture (ICA).
CreditCheckShortConnection	Emulates transactions that make a series of credit approvals. Creates a separate connection for each script transaction.
DatabaseUpdateShortConnect	Emulates updating a record in a database.
DNSNameLookup	Emulates performing a name lookup on a DNS server.
ExchangeDirectoryService	Emulates accessing the Microsoft Exchange Directory.
ExchangeReadMail	Emulates retrieving email from an Exchange server.
ExchangeReceiveMail	Emulates receiving periodic new mail notification from an Exchange server.
ExchangeSendMail	Emulates sending email from an Exchange client to the server.
FileReceiveShortConnection	Emulates requesting a file and receiving it.
FileSendShortConnection	Emulates sending a file and receiving an acknowledgment.
FTPGet	Emulates an FTP GET.
FTPPut	Emulates an FTP PUT.
HeadlinerInitialLoad	Emulates an initial run of Headliner using default settings.
HeadlinerSubsequentUpdate	Emulates updating a Headliner channel.
HTTPGIFTransfer	Emulates traffic of an HTTP GIF transfer from a Web server to a Web browser.
HTTPSSecureTransaction	Emulates HTTPS secure transfer of text or graphics between a Web server and a Web browser using SSL.
HTTPTextTransfer	Emulates traffic of an HTTP text transfer from a Web server to a Web browser.
InquiryShortConnection	Emulates typical client/server inquiry and reply.
LDAPDirectoryLookup	Emulates performing a lookup in an LDAP directory.

Knowledge Script	What It Does
MicrosoftRDPExcelStartUp	Emulates Excel startup on a Microsoft remote desktop using RDP.
MicrosoftRDPIEStartLoadMSN	Emulates starting and loading MSN Explorer on a Microsoft remote desktop using RDP.
MicrosoftRDPOutlookOpenBox	Emulates opening an Outlook box on a Microsoft remote desktop using RDP.
MicrosoftRDPTermServerLogon	Emulates logon to a Microsoft remote desktop using Terminal Services.
MicrosoftRDPWordStartUp	Emulates starting MS Word on a Microsoft remote desktop using RDP.
MSSQLQuery	Emulates queries to the SQL server.
NetworkNewsTransferProtocol	Emulates typical Usenet news reader activities using NNTP.
NotesAttachOpenDB	Emulates opening a document with an attachment in a Lotus Notes database.
NotesAttachOpenInitDB	Emulates opening a document with an attachment in a Lotus Notes database that you initialize.
NotesAttachServerDetach	Emulates doing a Lotus Notes server attachment and detachment.
NotesAttachServers2Detach	Emulates doing multiple server attachments and detachments.
NotesBrowserDBAttach	Emulates using a Lotus Notes browser to do an attach.
NotesBrowserDBOpen	Emulates using a Lotus Notes browser to do a database open.
NotesBrowserDBSearch	Emulates using a Lotus Notes browser to do a database search.
NotesCheckForUnreadEmail	Emulates Lotus Notes client periodically checking server for new mail.
NotesCreateSaveMailNote	Emulates Lotus Notes client creating, then saving an email message.
NotesCreateSaveSendAttach	Emulates a Lotus Notes client creating, saving, and sending a mail message with an attachment.
NotesCreateSaveSendMailNote	Emulate a Lotus Notes client creating, saving, and sending a mail message.
NotesCreateTextIndexServer	Emulates creating a text index on the Lotus Notes server.
NotesIndexedDBLookup	Emulates performing an indexed Lotus Notes database lookup.
NotesNonIndexedDBLookup	Emulates performing a non-indexed Lotus Notes database lookup.
NotesReceiveEmail	Emulates mail receipt by a Lotus Notes client.
NotesReplicateMail	Emulates replicating a Lotus Notes mail database.
NotesReplicateServer1DB	Emulates replicating one database in Lotus Notes.
NotesReplicateServer50Auto	Emulates Lotus Notes replication.
NotesReplicateServer50Docs	Emulates Lotus Notes replication of 50 documents.
NotesReplicateServerCheck	Emulates replicating a Lotus Notes server check.

Knowledge Script	What It Does
NotesSendEmail	Emulates a Lotus Notes client sending email to the server.
NTFilePrintPrintaFile	Emulates a Windows client requesting a print server to print a file.
OracleAPTier1FindInvoice	Emulates traffic between end user computer and the Tier 1 application server when finding an Accounts Payable invoice.
OracleAPTier1InvoiceMultDist	Emulates traffic between end user computer and the Tier 1 application server when handling multiple distribution of an invoice.
OracleAPTier2FindInvoice	Emulates traffic between the application server and the database server when finding an Accounts Payable invoice.
OracleAPTier2InvoiceMultDist	Emulates traffic between the application server and the database server when handling an Accounts Payable invoice.
OracleARTier1InsertCustomer	Emulates traffic between the end user computer and the Tier 1 application server when adding an Accounts Receivable customer.
OracleARTier1ViewCustomer	Emulates traffic between the end user computer and the Tier 1 application server when viewing an Accounts Receivable customer.
OracleARTier2InsertCustomer	Emulates traffic between the application server and the database server when adding a customer.
OracleARTier2ViewCustomer	Emulates traffic between the application server and the database server when viewing an Accounts Receivable customer.
OracleFATier1AssetInquiry	Emulates traffic between the end user computer and the Tier 1 application server when making a Fixed Assets asset inquiry.
OracleFATier1ManualAddition	Emulates traffic between the end user computer and the Tier 1 application server when doing a Fixed Assets manual addition.
OracleFATier2AssetInquiry	Emulates traffic between the application server and the database server when doing a Fixed Assets asset inquiry.
OracleFATier2ManualAddition	Emulates traffic between the application server and the database server when doing a Fixed Assets manual addition.
OracleGLTier1AccountInquiry	Emulates traffic between the end user computer and the Tier 1 application server when making a General Ledger account inquiry.
OracleGLTier1JournalEntry	Emulates traffic between the end user computer and the Tier 1 application server when making a General Ledger journal entry.
OracleGLTier2AccountInquiry	Emulates making a General Ledger account inquiry on an Oracle Tier 2 server.
OracleGLTier2JournalEntry	Emulates making a General Ledger journal entry on an Oracle Tier 2 server.
PacketBlasterLongConnection	Continuously sends packets from Endpoint 1 to Endpoint 2 using a long connection.
PacketBlasterRevLongConnect	Continually receives packets at Endpoint 1 using a long connection, without waiting for any response.

Knowledge Script	What It Does
PointCastv1InitialUpdate	Emulates a user getting an update of default content selections for PointCast Network version 1.
PointCastv2InitialUpdate	Emulates a user getting an update of default content selections for PointCast Network version 2.
POP3ReceiveEmail	Emulates email receipt using POP3 standard.
SAPR3AuthPaymentOnInvoice	Emulates payment authorization for an invoice.
SAPR3BasicStock	Emulates basic stock network transactions in SAPR3.
SAPR3BatchCharacterizeStock	Emulates stock characterization in SAP R/3.
SAPR3CreatePurchaseOrder	Emulates creation of a purchase order by an SAP R/3 operator at the client.
SAPR3CreateSalesOrder	Emulates creation of a sales order by an SAP R/3 operator at the client.
SAPR3GoodsReceipt	Emulates receipt of goods by an SAP R/3 operator at the client.
SAPR3GoodsReceiptInspection	Emulates a goods receipt inspection transaction by an SAP R/3 operator at the client.
SAPR3Login	Emulates a client login to an SAP R/3 server.
SAPR3MaterialToMaterialXfer	Emulates an SAP R/3 material transfer.
SAPR3PickingBatchDetermine	Emulates an SAP R/3 picking batch determination.
SAPR3PostGoods	Emulates posting goods by an SAP R/3 operator at the client.
SAPR3PrepareAnInvoice	Emulates invoice preparation based on a purchase order created using SAPpuror.
SAPR3QMResultsRecording	Emulates recording SAP R/3 QM module results by an SAP R/3 operator at the client.
SAPR3SalesOrderDelivery	Emulates a sales order delivery transaction by an SAP R/3 operator at the client.
SMTPSendEmail	Emulates sending email messages using TCP/IP's SMTP standard.
Telnet	Emulates a TCP/IP Telnet session.
Traceroute	Collects traceroute data for a specified source and target location on demand, or at regularly scheduled intervals.
Report_ResponseTimeSummary	Summary report of availability and response time for Networks-RT Knowledge Scripts.
Report_ThroughputSummary	Summary report of availability and throughput for Networks-RT Knowledge Scripts.
Report_TracerouteException	Compares exception traceroute data against the averaged baseline traceroute statistics from the associated source and target locations.
Report_TracerouteProfile	Summary report of the averaged baseline traceroute statistics for a given source and target location combination, along with the last ten exception traceroutes for the pair.
Net-RT-Import_KSGenerator	Custom scripts imported using the KSGenerator.

[ResponseTime]

Use this Knowledge Script to check response time between a pair of endpoints.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view you select determine which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 100.

Description	How to Set It
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size	Enter the size in bytes for the reply. Default is 100.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

[Throughput]

Use this Knowledge Script to test network throughput.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Throughput
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT throughput

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when throughput is less than threshold?	Select the **Yes** check box to raise an event when measured throughput falls below the threshold you set. By default, events are enabled.
Select endpoints to run the test to	Select the endpoint names, separated by commas, where the test will run.
Throughput threshold	Set the minimum throughput. The units are set in the **Throughput units for threshold and data** parameter. When throughput falls below this value, an event is raised. On threshold events, the event message contains a breakdown of the total throughput.
Throughput units for threshold and data	Select the units from the list. “K” represents 1024; “k” represents 1000. “B” represents bytes; “b” represents bits. The choices are: • **KBps** 1,024 Bytes per second • **kBps** 1,000 Bytes per second • **Kbps** 1,024 bits per second (128 Bytes per second) • **kbps** 1,000 bits per second (125 Bytes per second) • **Mbps** 1,000,000 bits per second (125,000 Bytes per second) • **Gbps** 1,000,000,000 bits per second (125,000,000 Bytes per second) **Note** Data is stored as kbps in the database regardless of the threshold units you set here. However, when you run the Networks-RT_Throughput Report, you can specify the units that are used in the report.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.

Description	How to Set It
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
File size	Enter the number of bytes in the transferred file. Default is 100,000.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

Action_Traceroute

Use this Knowledge Script to collect exception traceroute data between a specified source and target location in response to an event in another Knowledge Script.

When you select this Action Knowledge Script to run automatically in association with another Knowledge Script job, you must specify the source and target locations of the traceroute as parameters. The source location must have the ResponseTime for Networks managed object installed and discovered.

To associate this action with a particular monitoring script:

1. Double-click the desired monitoring Knowledge Script. Click the **Actions** tab in the Properties dialog box.
2. Select **Action_Traceroute** from the list in the **Action** column.
3. The **Location** parameter must be set to "**MC**" (managed client). Otherwise, this action will create an error event and will not collect traceroute data when it is invoked.

Note
Although any managed client can be selected as the "Location," the ResponseTime for Networks managed object must be installed on the managed client.

Set the action "Type" value to "Repeat Event - 1" if you want a new traceroute to run at each event.

Note
The "Type" value is dependent on the settings for event collapsing and on the schedule of the associated Knowledge Script. If the Knowledge Script runs and raises events more often than the event collapsing interval (default is 20 minutes), the traceroute action will not occur at every event. A new child event must be raised for the action to be executed.

Example

Before you launch a Knowledge Script other than one of the Networks-RT scripts, double-click it to see its Properties dialog box. Click the **Actions** tab. Click **New** and select **Action_Traceroute** from the list. Then click **Properties** to specify the source location and target location for the traceroute. If an event is raised by the Knowledge Script, the Action_Traceroute Knowledge Script is launched automatically. It collects traceroute data between the source and target you selected and stores the traceroute data in the AppManager repository.

The traceroute data is associated with the event that triggered the traceroute. Run the Report_TracerouteException Knowledge Script to generate a report that compares the traceroute data collected for this event with the historical traceroute data for the associated source and target locations.

Resource Object

NT_MachineFolder

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Description	How to Set It
Traceroute source location	Select a ResponseTime for Networks node where the traceroute will originate. Specify only one source. Maximum length is 64 characters.
Traceroute target location	Select a node where the traceroute will finish—a ResponseTime for Networks node, some other AppManager node, an IP address, or a URL. Specify only one target. The script validates whether the source and target locations are the same; generates an error if they are identical. Maximum length is 64 characters.
Maximum number of hops	Set the maximum number of hops allowed before the traceroute is abandoned. Allowable values are integers 1-30. Default is 30.
Event when traceroute fails?	Select the **Yes** check box to raise events. By default, events are enabled.
Traceroute failed event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 20.

Action_TracerouteNetworks-RT

Use this Knowledge Script to collect exception traceroute data between a specified source and target location in response to an event in a separate Networks-RT Knowledge Script.

You do not have to specify source or target information when associating the action script with the Knowledge Script. This script automatically determines the source and target locations for the traceroute, based on the event details from the Knowledge Script.

To associate this action with a particular monitoring script:

1. Double-click the desired monitoring Knowledge Script. Click the **Actions** tab in the Properties dialog box.
2. Select **Action_Traceroute** from the list in the **Action** column.
3. The **Location** parameter must be set to "**MC**" (managed client). Otherwise, this action will create an error event and will not collect traceroute data when it is invoked.

Note
The ResponseTime for Networks managed object must be installed on the managed client.

Set the action "Type" value to "Repeat Event - 1" if you want a new traceroute to run at each event.

Note
The "Type" value is dependent on the settings for event collapsing and on the schedule of the associated Knowledge Script. If the Knowledge Script runs and raises events more often than the event collapsing interval (default is 20 minutes), the traceroute action will not occur at every event. A new child event must be raised for the action to be executed.

Example

Before you launch a Networks-RT Knowledge Script, double-click it and click the **Actions** tab on the Properties dialog box. Click **New**, and select **Action_TracerouteNetworks-RT** from the list. If an event is raised by the Knowledge Script, the Action_TracerouteNetworks-RT Knowledge Script is launched automatically. It collects traceroute data between the source and target locations associated with the event, and stores the traceroute data in the AppManager database.

The traceroute data is associated with the event that triggered the traceroute. Run the Report_TracerouteException Knowledge Script to generate a report that compares the traceroute data collected for this event with the historical traceroute data for the given pair of endpoints.

Resource Object

Networks-RT

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Description	How to Set It
Maximum number of hops	Set the maximum number of hops allowed before the traceroute is abandoned. Default is 30.
Event when traceroute fails?	Select the **Yes** check box to raise events. By default, events are enabled.
Traceroute failed event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 20.

ActiveDirectoryAddUser

Use this Knowledge Script to emulate adding a user to a domain in the Active Directory.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability--Returns one of two values:
  - 1 ~ the test was successful
  - 0 ~ the test was not successful

An event is raised whenever one of the following occurs:

- A threshold is exceeded.
- A test fails because of a service availability failure.
- Any other error.

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify the maximum response time allowed before an event is raised. The event message contains a breakdown of the total response time. Required, unless threshold events are disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. This value is ignored if events are disabled.
Detailed Parameters	
Transactions per record	Enter the number of transactions to be entered per timing record. Default is 5.

Description	How to Set It
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Number of users	Enter the number of users added at one time. Default is 1.
User data	Enter the amount of data sent for one user in the group. Default is 3500.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

ActiveDirectoryLogin

Use this Knowledge Script to emulate the data flows generated when a user logs in from a Windows 2000 Professional computer to a Windows 2000 Server computer. It is useful for determining the response time that a single user experiences when attempting to log in to a domain controller.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view you select determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the test event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

ActiveDirectoryReplication

Use this Knowledge Script to emulate the network traffic generated between two computers during the full replication of a domain directory.

Editing the **Objects loop** and **Transfer amount** variables determines the number of times script commands are repeated. The values of these variables should depend on the number of object in a directory. The `objects_loop`, which controls the number of times the script commands are performed, increases by 2 for every 60 additional objects. When emulating 200 objects or fewer, the `transfer_amount` increases by 40,000 bytes for every 60 additional objects; with quantities of 200 objects or more, the `transfer_amount` increases by 20,000 bytes for every 60 additional objects. The following table provides an illustration:

Number of Objects	Script Variable Objects_Loop	Transfer Amount
60	8	580,000 bytes
120	10	620,000 bytes
180	12	660,000 bytes
480	22	760,000 bytes

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.

Description	How to Set It
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Transfer amount	Set the average amount of data transferred for each `SEND` in a directory replication. When you change this value for a number of users, also change the Objects loop variable. Default is 580,000.
Objects loop	Enter the number of objects transferred in a full directory replication from one domain controller to another. The default of 8 represents 60 objects. When you change this value, also change the Transfer amount variable.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

ActiveDirectoryResetPassword

Use this Knowledge Script to emulate the data flows that occur when you reset a user's password.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

BaanAddItem

Use this Knowledge Script to emulate the Baan function of adding an item to the Baan database.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

BaanGenerateMPSMRPBatches

Use this Knowledge Script to emulate the Baan function of generating Baan MPS MRP batches.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

BaanLoadDEM

Use this Knowledge Script to emulate the Baan function of loading Baan Dynamic Enterprise Management framework (DEM). This framework supports Baan implementation by using best-practice "Target" implementation methodology.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. he view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

BaanLoadItemMaster

Use this Knowledge Script to emulate the Baan function of loading Baan Item Master.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ the test was successful
  - 0 - the test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. Simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

BaanMaintainCustomer

Use this Knowledge Script to emulate the Baan function of maintaining a customer in Baan.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. Simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

BaanMaintainEmployeeAdd

Use this Knowledge Script to emulate the Baan function of adding an employee.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. Simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment.

BaanMaintainProductBom

Use this Knowledge Script to emulate the Baan function of maintaining a standard Baan Bill of Materials (BOM).

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. Simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

BaanMaintainPurchaseOrder

Use this Knowledge Script to emulate the Baan function of maintaining a purchase order.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. Simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

BaanMaintainSalesOrder

Use this Knowledge Script to emulate the Baan function of maintaining a sales order.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. Simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

BaanMaintainServiceOrder

Use this Knowledge Script to emulate the Baan function of maintaining a service order in the Baan system.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

BaanPrintCompaniesListSelect

Use this Knowledge Script to emulate the Baan function of printing a selected list of companies in the Baan system.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

BackWebSignupAndInfoPakDnld

Use this Knowledge Script to emulate subscribing to and downloading the contents of a new Back Web channel.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 300.
File size	Enter the number of bytes in the transferred file. Default is 3,000.

Description	How to Set It
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. Simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

BackWebUpdate

Use this Knowledge Script to emulate updating an existing Back Web channel.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 400.
File size	Enter the number of bytes in the transferred file. Default is 11,000.

Description	How to Set It
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

CastanetChannelDownload

Use this Knowledge Script to emulate the downloading of channels. Each timing record represents a single channel download. The default file size is 500,000 bytes; however, this value depends on the channel that is being downloaded.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 300.

Description	How to Set It
Reply size	Enter the number of bytes in the reply. Default is 2,000.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
File control size	Enter the size of the file control information to be sent and received, in preparation for transferring the file. In a real file transfer, this usually consists of directory and filename information. Default is 1500.
File size	Enter the number of bytes in the transferred file. Default is 500,000.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

CastanetInitialRun

Use this Knowledge Script to emulate a user running the Castanet Tuner for the first time. When running, this Tuner checks to verify that it is up-to-date by querying the Marimba home base. Next, it downloads the portion of the Java-based Tuner that is not up-to-date.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 300.

Description	How to Set It
Reply size	Enter the number of bytes in the reply. Default is 2,000.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
File control size	Enter the number of bytes that are in the control flows. Default is 1500.
File size	Enter the number of bytes in the transferred file. Default is 1,350,000.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

ccMail

Use this Knowledge Script to emulate sending a ccMail message.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. Simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

CitrixICAExcelStartup

Use this Knowledge Script to emulate starting up Excel within the Citrix Independent Computer Architecture (ICA).

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

CitrixICAIEStartup

Use this Knowledge Script to emulate starting up Internet Explorer within the Citrix Independent Computer Architecture (ICA).

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

CitrixICAOutlookOpenFullBox

Use this Knowledge Script to emulate opening Outlook within the Citrix Independent Computer Architecture (ICA).

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

CitrixICATerminalServerLogon

Use this Knowledge Script to emulate a terminal server logon within the Citrix Independent Computer Architecture (ICA).

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

CitrixICAWordStartUp

Use this Knowledge Script to emulate starting up MS Word within the Citrix Independent Computer Architecture (ICA).

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

CreditCheckShortConnection

Use this Knowledge Script to emulate transactions that make a series of credit approvals. Each record is sent from Endpoint 1; Endpoint 2 receives the record and sends back a confirmation. This script uses *short* connections: it creates a separate connection for each transaction in the script.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 100.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

DatabaseUpdateShortConnect

Use this Knowledge Script to emulate requesting a record from Endpoint 2, getting and updating the record, and sending it back. Endpoint 1 receives a confirmation that the update was completed. This script uses *short* connections: it creates a separate connection for each transaction in the script.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 100.

Description	How to Set It
Reply size	Enter the number of bytes in the reply. Default is 100.
Update size	Enter the number of bytes in the update. Default is 100.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

DNSNameLookup

Use this Knowledge Script to emulate looking up a name on the DNS server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
DNS answer size	Enter the number of bytes in the reply of the DNS server to the requesting client. Default is 150.
DNS question size	Enter the number of bytes in the DNS question request for the resolution of a name to an address. Default is 35.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

ExchangeDirectoryService

Use this Knowledge Script to emulate accessing the Microsoft Exchange Directory.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

ExchangeReadMail

Use this Knowledge Script to emulate retrieving email. Endpoint 1 (the client) requests the full list of unread email messages; Endpoint 2 (the server) sends the unread email messages to the client. You can change the Exchange mail size variable from 2800 to a value that more accurately represents the average email message size you are using in testing.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Exchange mail size	Enter the amount of bytes in the average email message. Default is 2800.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

ExchangeReceiveMail

Use this Knowledge Script to emulate a Microsoft Exchange client periodically receiving notification for new email. Endpoint 1 (the client) requests the list of unread email headers; Endpoint 2 (the server) sends this list to the client.

Note
The script does not include an 8-byte UDP message that the mail server sends to the client informing the client that a new message is on the server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	

Description	How to Set It
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

ExchangeSendMail

Use this Knowledge Script to emulate sending an email message from a Microsoft Exchange client to the server. The transaction only includes sending the message. Endpoint 2 (the server) acknowledges the message back to the Endpoint 1 (the client).

The default Exchange mail size of 1420 bytes includes 700 bytes of email control information; the remainder is text. You should always set this value to at least 700 bytes to include the email overhead.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	

Description	How to Set It
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Exchange mail size	Enter the number of bytes in the email message. Default is 1420.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

FileReceiveShortConnection

Use this Knowledge Script to emulate Endpoint 1 requesting a file, then receiving it. This script uses *short* connections: it creates a separate connection for each transaction in the script.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful
- Throughput

Resource Object

Networks throughput

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when throughput is less than threshold?	Select the **Yes** check box to raise an event when throughput falls below the threshold you set. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Throughput threshold	Set the minimum throughput. The units are set in the **Throughput units for threshold and data** parameter. When throughput falls below this value, an event is raised. On threshold events, the event message contains a breakdown of the total throughput.

Description	How to Set It
Throughput units for threshold and data	Select the units from the drop-list. “K” represents 1024; “k” represents 1000. “B” represents bytes; “b” represents bits. The choices are: • **KBps** 1,024 Bytes per second • **kBps** 1,000 Bytes per second • **Kbps** 1,024 bits per second (128 Bytes per second) • **kbps** 1,000 bits per second (125 Bytes per second) • **Mbps** 1,000,000 bits per second (125,000 Bytes per second) • **Gbps** 1,000,000,000 bits per second (125,000,000 Bytes per second) **Note** Data is stored as kbps in the database regardless of the threshold unit you set here. However, when you run the Networks-RT_Throughput Report, you can specify the unit that displays on the report.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 100.
File size	Enter the number of bytes in the transferred file. Default is 100,000.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

FileSendShortConnection

Use this Knowledge Script to emulate Endpoint 1 sending a file to Endpoint 2 and receiving an acknowledgment. This script uses *short* connections: it creates a separate connection for each transaction in the script.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful
- Throughput

Resource Object

Networks throughput

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when throughput is less than threshold?	Select the **Yes** check box to raise an event when throughput falls below the threshold you set. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Throughput threshold	Set the minimum throughput. The units are set in the **Throughput units for threshold and data** parameter. When throughput falls below this value, an event is raised. On threshold events, the event message contains a breakdown of the total throughput.

Description	How to Set It
Throughput units for threshold and data	Select the units from the drop-list. “K” represents 1024; “k” represents 1000. “B” represents bytes; “b” represents bits. The choices are: • **KBps** 1,024 Bytes per second • **kBps** 1,000 Bytes per second • **Kbps** 1,024 bits per second (128 Bytes per second) • **kbps** 1,000 bits per second (125 Bytes per second) • **Mbps** 1,000,000 bits per second (125,000 Bytes per second) • **Gbps** 1,000,000,000 bits per second (125,000,000 Bytes per second) **Note** Data is stored as kbps in the database regardless of the threshold unit you set here. However, when you run the Networks-RT_Throughput Report, you can specify the unit that displays on the report.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
File size	Enter the number of bytes in the transferred file. Default is 100,000.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

FTPGet

Use this Knowledge Script to emulate receiving a file at Endpoint 1 from Endpoint 2, using TCP/IP's FTP application (the `GET` function).

This script consists of three sections; each has its own connection. The first section emulates a logon by Endpoint 2 to Endpoint 1. The second section, the only one that is timed, emulates the transfer of a 100,000-byte file. The third section emulates a user logoff. Most variables in the first and third sections are hardcoded; these sections are components of the total network traffic that a real FTP transaction creates, but they are not in the timed loop.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful
- Throughput

Resource Object

Networks throughput

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when throughput is less than threshold?	Select the **Yes** check box to raise an event when throughput falls below the threshold you set. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Throughput threshold	Set the minimum throughput. The units are set in the **Throughput units for threshold and data** parameter. When throughput falls below this value, an event is raised. On threshold events, the event message contains a breakdown of the total throughput.

Description	How to Set It
Throughput units for threshold and data	Select the units from the drop-list. “K” represents 1024; “k” represents 1000. “B” represents bytes; “b” represents bits. The choices are: • **KBps** 1,024 Bytes per second • **kBps** 1,000 Bytes per second • **Kbps** 1,024 bits per second (128 Bytes per second) • **kbps** 1,000 bits per second (125 Bytes per second) • **Mbps** 1,000,000 bits per second (125,000 Bytes per second) • **Gbps** 1,000,000,000 bits per second (125,000,000 Bytes per second) **Note** Data is stored as kbps in the database regardless of the threshold unit you set here. However, when you run the Networks-RT_Throughput Report, you can specify the unit that displays on the report.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 100,000.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
File control size	Enter the size of the file control information to be sent and received, in preparation for transferring the file. In a real file transfer, this usually consists of directory and filename information. Default is 30.
Login size	Enter the number of bytes in the login flows.Default is 15.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

FTPPut

Use this Knowledge Script to emulate sending a file from Endpoint 1 to Endpoint 2 using the TCP/IP FTP application (the `PUT` function).

This script consists of three sections; each has its own connection. The first section emulates a logon by Endpoint 1 to Endpoint 2. The second section, the only one that is timed, emulates the transfer of a 100,000-byte file. The third section emulates a user logoff. Most variables in the first and third sections are hardcoded; these sections are components of the total network traffic that a real FTP transaction creates, but they are not in the timed loop.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful
- Throughput

Resource Object

Networks throughput

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when throughput is less than threshold?	Select the **Yes** check box to raise an event when throughput falls below the threshold you set. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Throughput threshold	Set the minimum throughput. The units are set in the **Throughput units for threshold and data** parameter. When throughput falls below this value, an event is raised. On threshold events, the event message contains a breakdown of the total throughput.

Description	How to Set It
Throughput units for threshold and data	Select the units from the drop-list. “K” represents 1024; “k” represents 1000. “B” represents bytes; “b” represents bits. The choices are: • **KBps** 1,024 Bytes per second • **kBps** 1,000 Bytes per second • **Kbps** 1,024 bits per second (128 Bytes per second) • **kbps** 1,000 bits per second (125 Bytes per second) • **Mbps** 1,000,000 bits per second (125,000 Bytes per second) • **Gbps** 1,000,000,000 bits per second (125,000,000 Bytes per second) **Note** Data is stored as kbps in the database regardless of the threshold unit you set here. However, when you run the Networks-RT_Throughput Report, you can specify the unit that displays on the report.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 100,000.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
File control size	Enter the size of the file control information to be sent and received, in preparation for transferring the file. In a real file transfer, this usually consists of directory and filename information. Default is 30.
Login size	Enter the number of bytes in the login flows. Default is 15.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

HeadlinerInitialLoad

Use this Knowledge Script to emulate the initial run of Headliner, using its default settings. Five channels are automatically selected. The list of channels is downloaded, in addition to the channel contents. Because the connections are not all serialized, the set of connections needs to be spread over a set of endpoint connections. Each channel is downloaded independently of the others.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 300.

Description	How to Set It
File size	Enter the number of bytes in the transferred file. Default is 15,000.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

HeadlinerSubsequentUpdate

Use this Knowledge Script to emulate the updating of a Headliner channel. In this script, the list of channels is not downloaded again as it is in HeadlinerInitialLoad. When new channels become available, the list of channels is then downloaded; however, this is not reflected in this emulation because this does not occur at a known time.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 300.

Description	How to Set It
File size	Enter the number of bytes in the transferred file. Default is 15,000.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

HTTPGIFTransfer

Use this Knowledge Script to emulate the traffic of an HTTP graphical image file (GIF) transfer from a Web server to a Web browser. Endpoint 1 (the client) requests a GIF file from Endpoint 2 (the server).

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 300.
File size	Enter the size of the transferred file. Default is 10,000.

Description	How to Set It
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

HTTPSSecureTransaction

Use this Knowledge Script to emulate an HTTPS secure text or graphics transfer between a Web server and a Web browser using SSL. The default values for the user data and response sizes reflect those commonly found in current Web browsers and servers.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User data size	Enter the number of bytes of user data that is sent to the secure transaction server. Examples of this type of information include: name, password, email address, contact address, etc. Default is 1,000.
Response size	Enter the number of bytes in the response. Default is 5,000.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

HTTPTextTransfer

Use this Knowledge Script to emulate traffic on an HTTP text transfer from a Web server to a Web browser.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 300.
File size	Enter the number of bytes in the transmitted file. Default is 1,000.

Description	How to Set It
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

InquiryShortConnection

Use this Knowledge Script to emulate a typical client/server inquiry transaction.

This script uses *short* connections: it creates a separate connection for each transaction in the script.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 100.

Description	How to Set It
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size	Enter the number of bytes in the reply. Default is 100.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

LDAPDirectoryLookup

Use this Knowledge Script to emulate a directory lookup in an LDAP directory.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

MicrosoftRDPExcelStartUp

Use this Knowledge Script to emulate starting up Excel on a Microsoft remote desktop that uses RDP.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

MicrosoftRDPIEStartLoadMSN

Use this Knowledge Script to emulate starting and loading MSN Explorer on a Microsoft remote desktop that uses RDP.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

MicrosoftRDPOutlookOpenBox

Use this Knowledge Script to emulate opening Outlook on a remote desktop that uses Microsoft RDP.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

MicrosoftRDPTermServerLogon

Use this Knowledge Script to emulate logon to a Microsoft remote desktop via Terminal Services.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

MicrosoftRDPWordStartUp

Use this Knowledge Script to emulate starting MS Word on a remote desktop that uses RDP.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

MSSQLQuery

Use this Knowledge Script to emulate a query to a SQL server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
Query string size	Enter the number of bytes in the query string. Default is 500.
Query result size	Enter the number of bytes in the query result. Default is 20,000.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

NetworkNewsTransferProtocol

Use this Knowledge Script to emulate activities on a typical Usenet news reader using NNTP. The script assumes that a typical user acts as follows: starts the news reader, opens a news server, selects a newsgroup about every 5-10 minutes, and reads a message about once every 10-60 seconds. Endpoint 1 emulates the news reader and Endpoint 2 emulates the news server.

The well-known port number for NNTP flows in TCP/IP is 119.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	

Description	How to Set It
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Server info size	Enter the size of the server ID message, in bytes, to be sent and received in preparation for transferring news articles. Default is 25.
Size of record to send	Enter the number of bytes to send in a record Default is 25.
Reply size	Enter the number of bytes in the reply. Default is 25.
Header response size	Enter the size of the article header, in bytes, to be sent and received. Default is 500.
Article response size	Enter the number of bytes in the article. Default is 1500.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Number of groups	Enter the number of groups to be retrieved. Default is 10.
Number of articles	Enter the number of articles to be retrieved. Default is 10.
Group delay	Enter a value to simulate user delay or processing between groups. The value can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)` where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Article delay	Enter a floating point number in seconds for the pause between articles.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

NotesAttachOpenDB

Use this Knowledge Script to emulate opening a document with an attachment in a Lotus Notes database.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response Time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

NotesAttachOpenInitDB

Use this Knowledge Script to emulate opening a document with an attachment in a Lotus Notes database that you initialize.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

NotesAttachServerDetach

Use this Knowledge Script to emulate doing an attachment and a detachment.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

NotesAttachServers2Detach

Use this Knowledge Script to emulate performing multiple server attachments and detachments.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

NotesBrowserDBAttach

Use this Knowledge Script to emulate using a Lotus Notes browser to perform an attach.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. Default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

NotesBrowserDBOpen

Use this Knowledge Script to emulate using a Lotus Notes browser to perform a database open.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

NotesBrowserDBSearch

Use this Knowledge Script to emulate a using a Lotus Notes browser to perform a database search.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

NotesCheckForUnreadEmail

Use this Knowledge Script to emulate a Lotus Notes client periodically checking for new email. Endpoint 1 (the client) requests the list of unread email "headers" (sender and subject); Endpoint 2 (the server) sends the list of unread email headers to the client.

The well-known port number for Lotus Notes flows in TCP/IP is 1352.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
File control size	Enter the number of bytes for the file control information to be sent and received in preparation for transferring the file. In an actual file transfer, this usually consists of the directory and filename information. Default is 100.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size	Enter the number of bytes in the reply. Default is 1,000.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

NotesCreateSaveMailNote

Use this Knowledge Script to emulate creating, then saving a Lotus Notes email message.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

NotesCreateSaveSendAttach

Use this Knowledge Script to emulate creating, saving, and sending a Lotus Notes email note with an attachment.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default `AUTO` for automatic assignment. Must be an integer between 1 and 65,535.

NotesCreateSaveSendMailNote

Use this Knowledge Script to emulate creating and sending a Lotus Notes email note and saving the message.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

NotesCreateTextIndexServer

Use this Knowledge Script to emulate creating a text index on the Lotus Notes server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

NotesIndexedDBLookup

Use this Knowledge Script to emulate performing an indexed Lotus Notes database lookup.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

NotesNonIndexedDBLookup

Use this Knowledge Script to emulate performing a non-indexed Lotus Notes database lookup.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

NotesReceiveEmail

Use this Knowledge Script to emulate email receipt by a Lotus Notes client. Each transaction represents the transfer of an email message from the server to the client. Endpoint 1 (the client) requests an email; Endpoint 2 (the server) sends it back to the client.

The default email message size, 2,000 bytes, includes 1,000 bytes of Lotus Note email control information and 1,000 bytes of readable text. You should therefore set this variable at no less than 1,000 bytes.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	

Description	How to Set It
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
File control size	Enter the number of bytes for the file control information to be sent and received in preparation for transferring the file. (In an actual file transfer, this usually consists of the directory and filename information. Default is 50.
File size	Enter the number of bytes in the email message to be transferred. Default is 2,000.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

NotesReplicateMail

Use this Knowledge Script to emulate replicating a Lotus Notes mail database.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

NotesReplicateServer1DB

Use this Knowledge Script to replicate one database.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

NotesReplicateServer50Auto

Use this Knowledge Script to emulate Notes replication.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

NotesReplicateServer50Docs

Use this Knowledge Script to emulate replicating 50 documents.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

NotesReplicateServerCheck

Use this Knowledge Script to emulate replicating a server check.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

NotesSendEmail

Use this Knowledge Script to emulate a Lotus Notes client sending email. Each transaction represents the transfer of an email message from the client to the server. Each transaction includes both the lookup of the recipient's name on the Lotus Notes local network database and the actual email message.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
File control size	Enter the number of bytes for the file control information to be sent and received in preparation for transferring the file. (In an actual file transfer, this usually consists of the directory and filename information. Default is 25.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
File size	Enter the number of bytes in the email message. Default is 2,000.
Reply size	Enter the number of bytes in the reply. Default is 100.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

NTFilePrintPrintaFile

Use this Knowledge Script to emulate a Windows client requesting a print server to print a file.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
Document loop	Default is 35.
Port number	Enter the port number, or use the default AUTO for automatic assignment.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleAPTier1FindInvoice

Use this Knowledge Script to replicate finding an Accounts Payable invoice. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the end user and computer and the application server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleAPTier1InvoiceMultDist

Use this Knowledge Script to emulate multiple distributions of an Accounts Payable invoice. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the end user and computer and the application server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleAPTier2FindInvoice

Use this Knowledge Script to emulate finding an Accounts Payable invoice. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the application server and the database server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleAPTier2InvoiceMultDist

Use this Knowledge Script to emulate multiple distributions of an Accounts Payable invoice. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the application server and the database server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleARTier1InsertCustomer

Use this Knowledge Script to emulate inserting an Accounts Receivable customer record. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the end user and computer and the application server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleARTier1ViewCustomer

Use this Knowledge Script to emulate viewing Accounts Receivable customer data. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the end user and computer and the application server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. Default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleARTier2InsertCustomer

Use this Knowledge Script to emulate inserting an Accounts Receivable customer record. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the application server and the database server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleARTier2ViewCustomer

Use this Knowledge Script to emulate viewing Accounts Receivable customer data. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the application server and the database server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleFATier1AssetInquiry

Use this Knowledge Script to emulate a Fixed Assets query into the Oracle Tier 1. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the end user and computer and the application server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleFATier1ManualAddition

Use this Knowledge Script to emulate making a Fixed Assets manual addition. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the end user and computer and the application server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers, then click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleFATier2AssetInquiry

Use this Knowledge Script to emulate making a Fixed Assets inquiry. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the application server and the database server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleFATier2ManualAddition

Use this Knowledge Script to emulate making a Fixed Assets manual addition. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the application server and the database server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleGLTier1AccountInquiry

Use this Knowledge Script to emulate a General Ledger inquiry. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the end user and computer and the application server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleGLTier1JournalEntry

Use this Knowledge Script to emulate making a General Ledger journal entry. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the end user and computer and the application server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleGLTier2AccountInquiry

Use this Knowledge Script to emulate making a General Ledger account inquiry. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the application server and the database server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

OracleGLTier2JournalEntry

Use this Knowledge Script to emulate making a General Ledger journal entry. If you deploy the application on separate servers for the application and database components, use this script to emulate traffic between the application server and the database server.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no delay). Can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

PacketBlasterLongConnection

Use this Knowledge Script to continuously send packets from Endpoint1 to Endpoint 2. This script uses a `long` connection; that is, it makes only one connection for the entire series of transactions in the script. There is no acknowledgment that data has been received. You may find this script helpful for generating background traffic.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes in the record to be sent. Default is 100.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

PacketBlasterRevLongConnect

Use this Knowledge Script to continually receive individual packets to Endpoint 1, as quickly as possible, without waiting for any response. Endpoint 1 thus has an exact record of how many bytes have been successfully received in each timing record. You may find this script helpful for generating background traffic.

This script uses a `long` connection; that is, it makes only one connection for the entire series of transactions in the script.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	

Description	How to Set It
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 100.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

PointCastv1InitialUpdate

Use this Knowledge Script to emulate a user getting an update of the default content selections for PointCast Network version 1. A record has 75 transactions, because about that many are required to download all the content.

Because each connection is serialized, only one endpoint connection is necessary. Each connection is made up of a request from client to server, and a response, which contains the requested content.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	

Description	How to Set It
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 150.
File size	Enter the number of bytes in the transferred file. Default is 15,000.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

PointCastv2InitialUpdate

Use this Knowledge Script to emulate a user getting an update of the default content selections for PointCast Network version 2. Some connections occur in parallel and others in serial. Up to five connections occur in parallel; therefore, five identical endpoint connections are needed, with 25 transactions per record, to download all the contents.

Because each connection is serialized, only one endpoint connection is necessary. Each connection is made up of a request from client to server, and a response, which contains the requested content.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	

Description	How to Set It
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 250.
File size	Enter the number of bytes in the transferred file. Default is 10,000.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

POP3ReceiveEmail

Use this Knowledge Script to emulate receipt of email messages using TCP/IP's POP3 standard. The script has three sections.

In the first section, Endpoint 1 receives a logon request, and replies by sending a user name. It then receives a request for and sends the associated password. Next, it receives the acknowledgment of a successful logon. Finally, it sends a request for the number of available email messages and receives the response.

In the second section's inner loop, Endpoint 1 sends a request for a specific email message. It then receives the message header, followed by the message body. Next, it sends a request to delete the email message, and receives an acknowledgment. To emulate a user who receives a large number of mail messages in a single logon, increase the Transactions per record variable.

In the third section, Endpoint 1 sends a message that the transfer is complete, and receives an acknowledgment.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.

Description	How to Set It
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 6.
Reply size	Enter the number of bytes in the reply. Default is 20.
File size	Enter the sized of the file control information to be sent and received in preparation for transferring the file. In an actual file transfer, this usually consists of directory and filename information. Default is 1,000.
File control size	Enter the number of bytes that are in the control flows. Default is 70.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3AuthPaymentOnInvoice

Use this Knowledge Script to emulate authorizing payment on an invoice prepared using SAP R/3. Each transaction represents one payment authorization and invoice release.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 100.

Description	How to Set It
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size	Enter the number of bytes in the reply. Default is 600.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3BasicStock

Use this Knowledge Script to emulate a basic stock network transaction by an SAP R/3 operator at the client.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Delay before responding1	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Size of record to send1	Enter the number of bytes to send in a record. Default is 62.
Reply size1	Enter the number of bytes in the reply. Default is 1103.
User delay1	Specify a value to simulate a user delay: Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution (Uniform, Normal, Poisson, or Exponential) expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Size of record to send2	Enter the number of bytes to send in a record. Default is 89.
Delay before responding2	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size2	Enter the number of bytes in the reply. Default is 2111.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3BatchCharacterizeStock

Use this Knowledge Script to emulate stock characterization procedures by an SAP R/3 operator at the client.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Size of record to send1	Enter the number of bytes to send in a record. Default is 52.
Delay before responding1	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size1	Enter the number of bytes in the reply. Default is 1103.
Size of record to send2	Enter the number of bytes to send in a record. Default is 60.
Reply size2	Enter the number of bytes in the reply. Default is 2111.
Size of record to send3	Enter the number of bytes to send in a record. Default is 51.
Reply size3	Enter the number of bytes in the reply. Default is 1466.
Size of record to send4	Enter the number of bytes to send in a record. Default is 53.
Reply size4	Enter the number of bytes in the reply. Default is 2696.
Size of record to send5	Enter the number of bytes to send in a record. Default is 55.
Reply size5	Enter the number of bytes in the reply. Default is 1354.
Delay before responding2 *(also 3, 4, and 5)*	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Client delay1 *(also 2, 3, and 4)*	Enter a floating point number of seconds to simulate a delay or processing at the client side.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3CreatePurchaseOrder

Use this Knowledge Script to emulate the creation of a purchase order by an SAP R/3 operator at the client. Each transaction represents the transfer of one purchase order in the SAP system. Endpoint 1 (the client) sends a purchase order request; Endpoint 2 (the server) responds with order information.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 50.

Description	How to Set It
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size	Default is 1400.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3CreateSalesOrder

Use this Knowledge Script to emulate the creation of a sales order by an SAP R/3 operator at the client. Each transaction represents the transfer of one sales order in the SAP system. Endpoint 1 (the client) sends a sales order request; Endpoint 2 (the server) responds with order information.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Size of record to send1	Enter the number of bytes to send in a record. Default is 54.
Delay before responding1	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size1	Enter the number of bytes in the reply. Default is 265.
Size of record to send2	Enter the number of bytes to send in a record. Default is 45.
Reply size2	Enter the number of bytes in the reply. Default is 239.
Size of record to send3	Default is 47.
Reply size3	Enter the number of bytes in the reply. Default is 271.
Size of record to send4	Enter the number of bytes to send in a record. Default is 45.
Reply size4	Enter the number of bytes in the reply. Default is 249.
Size of record to send5	Enter the number of bytes to send in a record. Default is 52.
Reply size5	Enter the number of bytes in the reply. Default is 808.
Size of record to send6	Enter the number of bytes to send in a record. Default is 114.
Reply size6	Enter the number of bytes in the reply. Default is 1838.
Size of record to send7	Enter the number of bytes to send in a record. Default is 164.
Reply size7	Enter the number of bytes in the reply. Default is 298.
Size of record to send8	Enter the number of bytes to send in a record. Default is 62.
Reply size8	Enter the number of bytes in the reply. Default is 130.
Size of record to send9	Enter the number of bytes to send in a record. Default is 64.
Reply size9	Enter the number of bytes in the reply. Default is 1698.
Size of record to send10	Enter the number of bytes to send in a record. Default is 66.
Reply size10	Enter the number of bytes in the reply. Default is 1668.
Delay before responding2 *(also 3 through 9)*	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Control delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.

Description	How to Set It
Delay before responding10	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Client delay1 *(also 2 through 9)*	Enter a floating point number of seconds to simulate a delay or processing at the client side.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3GoodsReceipt

Use this Knowledge Script to emulate obtaining a receipt for goods purchased (GR) in the SAP R/3 system.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Size of record to send1	Enter the number of bytes to send in a record. Default is 52.
Delay before responding1	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size1	Enter the number of bytes in the reply. Default is 840.
Size of record to send2	Enter the number of bytes to send in a record. Default is 111.
Reply size2	Enter the number of bytes in the reply. Default is 1427.
Size of record to send3	Enter the number of bytes to send in a record. Default is 134.
Reply size3	Enter the number of bytes in the reply. Default is 1051.
Size of record to send4	Enter the number of bytes to send in a record. Default is 94.
Reply size4	Enter the number of bytes in the reply. Default is 1468.
Size of record to send5	Enter the number of bytes to send in a record. Default is 59.
Reply size5	Enter the number of bytes in the reply. Default is 878.
Delay before responding2 *(also 3 through 5)*	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Client delay1 *(also 2 through 4)*	Enter a floating point number of seconds to simulate a delay or processing at the client side.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3GoodsReceiptInspection

Use this Knowledge Script to emulate obtaining a goods inspection receipt by an SAP R/3 operator at the client.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Size of record to send1	Enter the number of bytes to send in a record. Default is 52.
Delay before responding1	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size1	Enter the number of bytes in the reply. Default is 844.
Size of record to send2	Enter the number of bytes to send in a record. Default is 103.
Reply size2	Enter the number of bytes in the reply. Default is 1427.
Size of record to send3	Enter the number of bytes to send in a record. Default is 135.
Reply size3	Enter the number of bytes in the reply. Default is 258.
Size of record to send4	Enter the number of bytes to send in a record. Default is 67.
Reply size4	Enter the number of bytes in the reply. Default is 128.
Size of record to send5	Enter the number of bytes to send in a record. Default is 67.
Reply size5	Enter the number of bytes in the reply. Default is 1056.
Size of record to send6	Enter the number of bytes to send in a record. Default is 94.
Reply size6	Enter the number of bytes in the reply. Default is 1470.
Size of record to send7	Enter the number of bytes to send in a record. Default is 59.
Reply size7	Enter the number of bytes in the reply. Default is 880.
Delay before responding2 *(also 3 through 7)*	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Client delay1 *(also 2 through 6)*	Enter a floating point number of seconds to simulate a delay or processing at the client side.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3Login

Use this Knowledge Script to emulate a login to an SAP R/3 server by operator at the client. Endpoint 1 (the SAP R/3 client) sends login and control messages to Endpoint 2 (the server).

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 100.

Description	How to Set It
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size	Enter the number of bytes in the reply. Default is 500.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3MaterialToMaterialXfer

Use this Knowledge Script to emulate an SAPR3 material to material transfer by an SAP R/3 operator at the client.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Size of record to send1	Enter the number of bytes to send in a record. Default is 52.
Delay before responding1	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size1	Enter the number of bytes in the reply. Default is 832.
Size of record to send2	Enter the number of bytes to send in a record. Default is 103.
Reply size2	Enter the number of bytes in the reply. Default is 1399.
Size of record to send3	Enter the number of bytes to send in a record. Default is 152.
Reply size3	Enter the number of bytes in the reply. Default is 577.
Size of record to send4	Enter the number of bytes to send in a record. Default is 119.
Reply size4	Enter the number of bytes in the reply. Default is 259.
Size of record to send5	Enter the number of bytes to send in a record. Default is 67.
Reply size5	Enter the number of bytes in the reply. Default is 128.
Size of record to send6	Enter the number of bytes to send in a record. Default is 67.
Reply size6	Enter the number of bytes in the reply. Default is 1038.
Size of record to send7	Enter the number of bytes to send in a record. Default is 95.
Reply size7	Enter the number of bytes in the reply. Default is 1488.
Size of record to send8	Enter the number of bytes to send in a record. Default is 59.
Reply size8	Enter the number of bytes in the reply. Default is 868.
Delay before responding2 *(also 3 through 8)*	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Client delay1 *(also 2 through 7)*	Enter a floating point number of seconds to simulate a delay or processing at the client side.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3PickingBatchDetermine

Use this Knowledge Script to emulate the process of determining a picking batch in SAP R/3.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
Size of record to send1	Enter the number of bytes to send in a record. Default is 45.
Delay before responding1	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size1	Enter the number of bytes in the reply. Default is 284.
Size of record to send2	Enter the number of bytes to send in a record. Default is 46.
Reply size2	Enter the number of bytes in the reply. Default is 198.
Size of record to send3	Enter the number of bytes to send in a record. Default is 47.
Reply size3	Enter the number of bytes in the reply. Default is 271.
Size of record to send4	Enter the number of bytes to send in a record. Default is 58.
Reply size4	Enter the number of bytes in the reply. Default is 1617.
Size of record to send5	Enter the number of bytes to send in a record. Default is 95.
Reply size5	Enter the number of bytes in the reply. Default is 176.
Size of record to send6	Enter the number of bytes to send in a record. Default is 58.
Reply size6	Enter the number of bytes in the reply. Default is 1803.
Size of record to send7	Enter the number of bytes to send in a record. Default is 58.
Reply size7	Enter the number of bytes in the reply. Default is 228.
Size of record to send8	Enter the number of bytes to send in a record. Default is 59.
Reply size8	Enter the number of bytes in the reply. Default is 1481.
Size of record to send9	Enter the number of bytes to send in a record. Default is 67.
Reply size9	Enter the number of bytes in the reply. Default is 1512.
Size of record to send10	Enter the number of bytes to send in a record. Default is 62.
Reply size10	Enter the number of bytes in the reply. Default is 1386.
Client delay1 *(also 2 through 9)*	Enter a floating point number of seconds to simulate a delay or processing at the client side.
Control delay1	Specify a value to simulate a client delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Loop reply1	Enter the number of bytes in the loop reply. Default is 185.
Loop client delay	Specify a value to simulate a client delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Loop reply2	Enter the number of bytes in the loop reply. Default is 1450.

Description	How to Set It
Loop server delay2	Specify a value to simulate a client delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Size of record to send11	Enter the number of bytes in the transmitted record. Default is 59.
Reply size11	Enter the number of bytes in the reply. Default is 1800.
Client delay10	Enter a floating point number of seconds to simulate a delay or processing at the client side.
Delay before responding11	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Loop size to send3	Enter the number of bytes in the loop file. Default is 85.
Loop reply3	Enter the number of bytes in the loop reply. Default is 332.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3PostGoods

Use this Knowledge Script to emulate the posting of goods in the SAP R/3 system by an operator at the client.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is generated. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Size of record to send1	Enter the number of bytes to send in a record. Default is 47.
Delay before responding1	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size1	Enter the number of bytes in the reply. Default is 667.
Size of record to send2	Enter the number of bytes to send in a record. Default is 59.
Reply size2	Enter the number of bytes in the reply. Default is 225.
Size of record to send3	Enter the number of bytes to send in a record. Default is 60.
Reply size3	Enter the number of bytes in the reply. Default is 577.
Size of record to send4	Enter the number of bytes to send in a record. Default is 58.
Reply size4	Enter the number of bytes in the reply. Default is 1727.
Size of record to send5	Enter the number of bytes to send in a record. Default is 95.
Reply size5	Enter the number of bytes in the reply. Default is 176.
Size of record to send6	Enter the number of bytes to send in a record.57.
Reply size6	Enter the number of bytes in the reply. Default is 1828.
Size of record to send7	Enter the number of bytes to send in a record.59.
Reply size7	Enter the number of bytes in the reply. Default is 224.
Size of record to send8	Enter the number of bytes to send in a record. Default is 67.
Reply size8	Enter the number of bytes in the reply. Default is 607.
Delay before responding2 *(also 3 through 8)*	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Client delay1 *(also 2 through 7)*	Enter a floating point number of seconds to simulate a delay or processing at the client side.
Control delay1	Specify a value to simulate a client delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3PrepareAnInvoice

Use this Knowledge Script to emulate the preparation of an invoice based on the purchase order created using SAPpuror. Each transaction represents one invoice transfer for payment in the SAP R/3 system. Endpoint 1 (the client) requests invoice and payment information; Endpoint 2 (the server) responds with a customer invoice.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 100.

Description	How to Set It
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size	Enter the number of bytes in the reply. Default is 1,000.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3QMResultsRecording

Use this Knowledge Script to emulate the recording of SAP R/3 QM module results by an operator at the client.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless “Event when threshold is exceeded” is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.

Description	How to Set It
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Size of record to send1	Enter the number of bytes to send in a record. Default is 59.
Delay before responding1	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size1	Enter the number of bytes in the reply. Default is 399.
Size of record to send2	Enter the number of bytes to send in a record. Default is 45.
Reply size2	Enter the number of bytes in the reply. Default is 265.
Size of record to send3	Enter the number of bytes to send in a record. Default is 46.
Reply size3	Enter the number of bytes in the reply. Default is 203.
Size of record to send4	Enter the number of bytes to send in a record. Default is 48.
Reply size4	Enter the number of bytes in the reply. Default is 399.
Size of record to send5	Enter the number of bytes to send in a record. Default is 46.
Reply size5	Enter the number of bytes in the reply. Default is 316.
Size of record to send6	Enter the number of bytes to send in a record. Default is 46.
Reply size6	Enter the number of bytes in the reply. Default is 1177.
Size of record to send7	Enter the number of bytes to send in a record. Default is 122.
Reply size7	Enter the number of bytes in the reply. Default is 873.
Size of record to send8	Enter the number of bytes to send in a record. Default is 53.
Reply size8	Enter the number of bytes in the reply. Default is 941.
Size of record to send9	Enter the number of bytes to send in a record. Default is 53.
Reply size9	Enter the number of bytes in the reply. Default is 2102.
Size of record to send10	Enter the number of bytes to send in a record. Default is 161.
Reply size10	Enter the number of bytes in the reply. Default is 1194.
Delay before responding2 *(also 3 through 10)*	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Client delay1 *(also 2 through 9)*	Enter a floating point number of seconds to simulate a delay or processing at the client side.
Control delay1 *(also 2)*	Specify a value to simulate a server delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.

Description	How to Set It
Size of loop record	Enter the number of bytes in the loop record.
Loop reply size	Enter the number of bytes in the loop reply.
Loop client delay	Specify a value to simulate a client delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Loop respond delay	Enter a floating point number of seconds for a delay at the loop endpoint.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SAPR3SalesOrderDelivery

Use this Knowledge Script to emulate the delivery of an SAP R/3 sales order by an operator at the client.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.

Description	How to Set It
Size of record to send1	Enter the number of bytes to send in a record. Default is 45.
Delay before responding1	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Reply size1	Enter the number of bytes in the reply. Default is 284.
Size of record to send2	Enter the number of bytes to send in a record. Default is 46.
Reply size2	Enter the number of bytes in the reply. Default is 860.
Size of record to send3	Enter the number of bytes to send in a record. Default is 58.
Reply size3	Enter the number of bytes in the reply. Default is 1838.
Size of record to send4	Enter the number of bytes to send in a record. Default is 164.
Reply size4	Enter the number of bytes in the reply. Default is 299.
Size of record to send5	Enter the number of bytes to send in a record. Default is 62.
Reply size5	Enter the number of bytes in the reply. Default is 130.
Size of record to send6	Enter the number of bytes to send in a record. Default is 63.
Reply size6	Enter the number of bytes in the reply. Default is 1699.
Size of record to send7	Enter the number of bytes to send in a record. Default is 95.
Reply size7	Enter the number of bytes in the reply. Default is 176.
Size of record to send8	Enter the number of bytes to send in a record. Default is 58.
Reply size8	Enter the number of bytes in the reply. Default is 228.
Size of record to send9	Enter the number of bytes to send in a record. Default is 57.
Reply size9	Enter the number of bytes in the reply. Default is 1803.
Size of record to send10	Enter the number of bytes to send in a record. Default is 59.
Reply size10	Enter the number of bytes in the reply. Default is 1481.
Delay before responding2 *(also 3 through 10)*	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Client delay1 *(also 2 through 9)*	Enter a floating point number of seconds to simulate a delay or processing at the client side.
Loop reply1	Enter the number of bytes in the loop reply. Default is 155.
Loop client delay	Specify a value to simulate a client delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Loop reply2	Enter the number of bytes in the loop reply. Default is 1450.

Description	How to Set It
Control delay2	Specify a value to simulate a server delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Loop client delay2	Specify a value to simulate a client delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Client delay10	Enter a floating point number of seconds to simulate a delay or processing at the client side.
Loop size to send3	Enter the number of bytes in the loop file. Default is 63.
Loop reply3	Enter the number of bytes in the loop reply. Default is 1575.
Control delay	Specify a value to simulate a server delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Client delay11	Enter a floating point number of seconds to simulate a delay or processing at the client side.
Size of record to send12	Enter the number of bytes to send in a record. Default is 123.
Reply size12	Enter the number of bytes in the reply. Default is 168.
Delay before responding12	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

SMTPSendEmail

Use this Knowledge Script to emulate the sending of email messages from Endpoint 1 to Endpoint 2, using TCP/IP's SMTP standard.

The response time will be faster if you use a file size that is larger than the underlying MTU size; for example, use 1461 bytes or larger on Ethernet. The default data type for the email message is `NEWS.CMP` (a file containing text resembling a news article). The script has three sections.

In the first section, Endpoint 1 establishes a connection with the SMTP server and sends the identity of the mail sender and receiver.

In the second section, Endpoint 1 sends the body of the email message. Note the "Size of record to send" variable.

In the third section, Endpoint 1 sends a message that the email message is complete, and receives an acknowledgment.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time. Required, unless "Event when threshold is exceeded" is disabled.

Description	How to Set It
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If you disable throughput events, this value is ignored.
Detailed Parameters	
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 40.
Reply size	Enter the number of bytes in the reply. Default is 10.
File size	Enter the number of bytes in the transmitted email message. Default is 1,000.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

Telnet

Use this Knowledge Script to emulate a TCP/IP Telnet session. Default values indicate that Endpoint 1 sends one byte of data to Endpoint 2, which replies by echoing the same one-byte record. Endpoint 1 contains a `SLEEP` inside the inner loop: `user_delay`. Set this sleep period to a non-zero value to approximate the time the users being emulated pause between keystrokes when typing. The default data type for the exchanged bytes is `TRANS.CMP`.

The well-known port number for Telnet flows in TCP/IP is 23.

If you choose to collect data, this Knowledge Script generates the following data streams:

- Response time
- Availability ~ Returns one of two values:
  - 1 ~ test was successful
  - 0 ~ test was not successful

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Event when test fails to run?	Select the **Yes** check box to raise an event when the test fails to run. By default, events are enabled.
Event when response time exceeds threshold?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are enabled.
Select endpoints to run the test to	Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**.
Response time threshold (seconds)	Specify a floating point number in seconds. When response time exceeds this value, an event is raised. On threshold events, the event message contains a breakdown of the total response time.
Unsuccessful test event severity	Set the severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15. If response time events are disabled, this value is ignored.
Detailed Parameters	

Description	How to Set It
Transactions per record	Enter a positive integer to represent the number of transactions to simulate. The value varies according to the application script.
Size of record to send	Enter the number of bytes to send in a record. Default is 1.
Delay before responding	Enter a number of seconds to simulate a server delay. Default is 0 (no delay). Before executing the next script, the server pauses for the specified value, which can be either a positive integer or a random distribution expressed in milliseconds. The format for random distributions is `r(l,u)`, where `r` = U (uniform), N (normal), P (poisson), or E (exponential); `l` = lower limit; u = upper limit. For example, `u(1,10)`.
User delay	Specify a value to simulate a user delay. Before executing the next command, the script pauses for the specified time. Default is 0 (no pause). The value can be a positive integer or random distribution expressed in milliseconds. The random distribution format is `r(l,u)`, where `r` = U (Uniform), N (Normal), P (Poisson), or E (Exponential); `l` = lower limit; `u` = upper limit. For example, `u(1,10)`.
Transaction delay	Enter a positive integer in milliseconds to control the frequency of transaction execution. This simulates an end user running the transaction on a regular basis. The default of 0 sets no delay, so that the script executes the number of transactions per record as quickly as possible.
Destination port	Enter the destination port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.
Source port	Enter the source port number, or use the default AUTO for automatic assignment. Must be an integer between 1 and 65,535.

Traceroute

Use this Knowledge Script to collect traceroute data for a specified source and target location on demand, or at regularly scheduled intervals.

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 4 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Select the **Yes** check box to collect traceroute data. By default, data is collected.
Event when traceroute fails?	Select the **Yes** check box to raise events. By default, events are enabled.
Event when total latency exceeds threshold?	Select the **Yes** check box to raise events. Default is n.
Select the traceroute target locations	Enter an AppManager ResponseTime for Networks node, some other AppManager node, an IP address, or a URL. The maximum length is 64 characters. **Note** The source location is the computer where the script is dropped. Click the **Browse [...]** button to display the **Select a View** dialog box. Highlight a view from the list and click **Next** to open the **Select Desired Computer(s)** dialog box. The view determines which computers are available for selection. Select one or more endpoint computers. Click **Finish**. Or specify multiple targets separated by commas in the text input field. The script validates whether at least one of the target locations is different from the source location where the script is dropped.
Maximum number of hops	Enter an integer, 1-30. Set the maximum number of hops allowed in the traceroute. Default is 30.
Total latency threshold (sec)	Set the threshold for the total latency in seconds. Default is 1.000 seconds. The latency threshold must not be blank if the **Event when total latency exceeds threshold?** parameter is enabled.
Traceroute failed event severity	Set the event severity, from 1 to 40, to indicate the importance of the event. Default is 15.
Threshold event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 25.

Example of How this Script Is Used

This script can be used to collect baseline traceroute data between a specified source and target location. This is particularly useful if you have also selected either the Action_TracerouteAction_Traceroute script or the Action_TracerouteNetworks-RTAction_TracerouteNetworks-RT script as an action associated with a separate Knowledge Script. If you are collecting exception traceroutes by means of an action traceroute script, the baseline data collected by the Networks-RT_Traceroute script may be used as a comparison with the exception data. However, for comparison of baseline and exception data, you must run the Networks-RT_Traceroute script against the same source and target location as the Knowledge Script(s) that might generate exception traceroutes.

In addition to comparing the Networks-RT_Traceroute data against exception data, the baseline data may also be viewed on its own. You may run the Report_TracerouteProfile script to generate a report that summarizes the accumulated traceroute data for a given source and target location thus far.

Report_ResponseTimeSummary

Use this Report Knowledge Script to generate a summary report detailing availability and response time for response time-specific Networks-RT Knowledge Scripts.

Note
This report replaces all of the ResponseTime reports included in previous releases. The following reports have been replaced:

- Report_ActiveDirectory
- Report_Baan
- Report_ccMail
- Report_Citrix
- Report_Exchange
- Report_Internet
- Report_LDAP
- Report_LotusNotes
- Report_MSRDP
- Report_MSSQL
- Report_Oracle
- Report_ResponseTime
- Report_SAPR3
- Report_WebPush
- Report_WindowsNT

Resource Object

AppManager repository

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.

Description	How to Set It
KS for report	Select the Knowledge Script to report on. Click the **Browse [...]** button to show the Filter KS List dialog box. Select one of the following: • **Show scripts where report data is currently available.** Displays a filtered list of scripts that have been previously executed and have generated report data streams. • **Show All Networks-RT scripts.** Displays all Network-RT scripts, including those with no associated data. Select this option if, for example, you are configuring reports for tests that have not yet started running. Click **OK** to show the Select a Knowledge Script dialog box. Highlight a Networks-RT script from the Knowledge Script Name list and click **Finish** to select it.
Endpoint 1 computer(s)	Select the Endpoint 1 computer(s). Click the **Browse [...]** button to show the Select View(s) and a filter dialog box. From the View(s) list, select from one to twenty-five views. Your subsequent selections are limited to computers or server groups that are visible in the selected views. Select one of the Filters options: • **View:** Includes all computers in the views you selected. • **Computer:** Select from individual computers in the views you selected. • **Server Group:** Select from server groups in the views you selected. Selecting a server group includes all computers in that group.
Endpoint 2 computer or “All”	Type the name of the Endpoint 2 computer, or type “All” to designate all computers as Endpoint 2 computers.
Select time range	In the Select Date/Time Range dialog box, set specific start and end report information dates (good for historical or ad hoc reports), or a sliding range (the default) that sets the time range of data to include in the report. This option is useful for reports running on a regular schedule and is the default.
Select peak weekday(s)	In the Select Peak Weekday(s) dialog box, press **Shift** to select a contiguous day range, or **Ctrl** to select non-contiguous days.
Aggregation by	Select the time unit by which to aggregate data. Default is Hour. Works in conjunction with the next field **Aggregation interval**, which determines the number of units for one interval of data aggregation.
Aggregation interval	Select the interval units in which to aggregate data. Default is 1. For example, if you aggregate by the Hour and select 1 here, data is aggregated once every hour.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter card?	Specify whether to display a table of parameters used in the report.
Include Availability detail table?	Specify whether to display the Availability detail table as part of the report. By default, the table is included.
Include Availability chart?	Specify whether to display the Availability chart as part of the report. By default, the chart is included.
Threshold on Availability chart	Enter an integer for the percent. Default is 0 (no threshold is displayed).
Include Response Time detail table?	Specify whether to display the Response Time detail table as part of the report. By default, the table is included.
Include Response Time chart?	Specify whether to display the Response Time chart as part of the report. By default, the chart is included.
Units for Response Time report	Select the response time unit of msec (the default) or sec.

Description	How to Set It
Threshold on Response Time chart (selected units)	Enter the units in seconds > 0, or use the default of 0.0. Zero suppresses the threshold indicator in the chart.
Select chart style	Options in the Chart Settings dialog box set the appearance of the chart. The same parameters are used in both the availability and response time charts, if both are produced. Default is Ribbon.
Select output folder	In the Specify report folder/filename dialog box, enter an output filename and fill in the remote folder fields.
Add job ID to output folder name?	Specify whether to append a job ID to the output folder name. By default, the job ID is not appended.
Index-Report Title	In the Report Properties dialog box, configure report title settings.
Add time stamp to title	Specify whether to add a timestamp to the report title.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Generate event on success?	Specify whether an event is raised when a report is generated. By default, events are enabled.
Severity level for report success	Set the severity level for a successful report. Default is 35.
Severity level for report with no data	Set the severity level for a report with no data. Default is 25.
Severity level for report failure	Set the severity level for a report with no data. Default is 5.

Report_ThroughputSummary

Use this Report Knowledge Script to generate a summary report detailing availability and throughput for the following Networks-RT scripts:

- [Throughput]
- FileReceiveShortConnection
- FileSendShortConnection
- FTPGet
- FTPPut

Resource Object

AppManager repository

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
KS for report	Select the Knowledge Script to report on. Click the **Browse [...]** button to show the Filter KS List dialog box. Select one of the following: • **Show scripts where report data is currently available.** Displays a filtered list of scripts that have been previously executed and have generated report data streams. • **Show All Networks-RT scripts.** Displays all Network-RT scripts, including those with no associated data. Select this option if, for example, you are configuring reports for tests that have not yet started running. Click **OK** to show the Select a Knowledge Script dialog box. Highlight a Networks-RT script from the Knowledge Script Name list and click **Finish** to select it.
Endpoint 1 computer(s)	Select the Endpoint 1 computer(s). Click the **Browse [...]** button to show the Select View(s) and a filter dialog box. From the View(s) list, select from one to twenty-five views. Your subsequent selections are limited to computers or server groups that are visible in the selected views. Select one of the Filters options: • **View:** Includes all computers in the views you selected. • **Computer:** Select from individual computers in the views you selected. • **Server Group:** Select from server groups in the views you selected. Selecting a server group includes all computers in that group.
Endpoint 2 computer or “All”	Type the name of the Endpoint 2 computer, or type “All” to designate all computers as Endpoint 2 computers.

Description	How to Set It
Select time range	In the Select Date/Time Range dialog box, set specific start and end report information dates (good for historical or ad hoc reports), or a sliding range (the default) that sets the time range of data to include in the report. This option is useful for reports running on a regular schedule and is the default.
Select peak weekday(s)	In the Select Peak Weekday(s) dialog box, press **Shift** to select a contiguous day range, or **Ctrl** to select non-contiguous days.
Aggregation by	Select the time unit by which to aggregate data. Default is Hour. Works in conjunction with the next field **Aggregation interval**, which determines the number of units for one interval of data aggregation.
Aggregation interval	Select the interval units in which to aggregate data. Default is 1. For example, if you aggregate by the Hour and select 1 here, data is aggregated once every hour.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter card?	Specify whether to display a table of parameters used in the report.
Include Availability detail table?	Specify whether to display the Availability detail table as part of the report. By default, the table is included.
Include Availability chart?	Specify whether to display the Availability chart as part of the report. By default, the chart is included.
Threshold on Availability chart	Enter an integer for the percent. Default is 0 (no threshold is displayed).
Include Throughput detail table?	Specify whether to display the Response Time detail table as part of the report. By default, the table is included.
Include Throughput chart?	Specify whether to display the Response Time chart as part of the report. By default, the chart is included.
Units for Throughput report	Select the units from the drop-list. “K” represents 1024; “k” represents 1000. “B” represents bytes; “b” represents bits. The choices are: • **KBps** 1,024 Bytes per second • **kBps** 1,000 Bytes per second • **Kbps** 1,024 bits per second (128 Bytes per second) • **kbps** 1,000 bits per second (125 Bytes per second) • **Mbps** 1,000,000 bits per second (125,000 Bytes per second) • **Gbps** 1,000,000,000 bits per second (125,000,000 Bytes per second)
Threshold on Throughput chart (selected units)	Enter the units in seconds > 0, or use the default of 0.0. Zero suppresses the threshold indicator in the chart.
Select chart style	Options in the Chart Settings dialog box set the appearance of the chart. The same parameters are used in both the availability and response time charts, if both are produced. Default is Ribbon.
Select output folder	In the Specify report folder/filename dialog box, enter an output filename and fill in the remote folder fields.
Add job ID to output folder name?	Specify whether to append a job ID to the output folder name. By default, the job ID is not appended.
Index-Report Title	In the Report Properties dialog box, configure report title settings.
Add time stamp to title	Specify whether to add a timestamp to the report title.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.

Description	How to Set It
Generate event on success?	Specify whether an event is raised when a report is generated. By default, events are enabled.
Severity level for report success	Set the severity level for a successful report. Default is 35.
Severity level for report with no data	Set the severity level for a report with no data. Default is 25.
Severity level for report failure	Set the severity level for a report with no data. Default is 5.

Report_TracerouteException

Use this Report Knowledge Script to generate a report that compares exception traceroute data collected in response to an event by means of an action traceroute script against the averaged traceroute statistics from the associated source and target locations.

The data used in the comparison will be from the two weeks immediately prior to the time the exception traceroute was collected.

Note
If an Action Traceroute fails, then the TracerouteException Report will NOT be able to create an Exception Report for the event that initiated the Action Traceroute. If the Action Traceroute fails, an event is raised to denote the failure.

Resource Object

Report Agent (with Networks-RT subfolder)

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameter to select the data for your report.
Event Id	Enter the event ID associated with the exception traceroute data to compare with the baseline traceroute data. The report checks whether traceroute data is associated with the event ID, and reports an error if there isn't any.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter card?	Select whether to include a table of report parameters at the end of the report. By default, the table is included.
Include traceroute analysis table?	Select whether to include comparison table of exception route vs. most common baseline route in the report. By default, the table is included.
Include route frequency table?	Select whether to include table of route frequencies in the report. By default, the table is included.
Include route details table?	Select whether to include route details table(s) in the report. By default, the table is included.
Include last 10 exception route tables?	Select whether to include last 10 exception route table(s) in the report. By default, the table is included.
Select output folder	Enter a report filename and folder. Default is "`Networks-RT_TracerouteException\default.htm`".

Add job ID to output folder name?	Select whether to append the report job ID to the report output folder name. By default, the job ID is not appended.
Index-Report Title	Choose report title, author, company, component, description, expiration period, and custom fields. Defaults: Title = Networks-RT Traceroute Exception Author = NetIQ AppManager Company = Your company here Component = NetIQ AppManager 5.0 Networks-RT Module Description = Reports for Networks-RT: Traceroute Exception Expiration Period = Expires after 7 days Custom Field 1 = Networks-RT Endpoint, Traceroute Exception Custom Field 2 = Exception traceroute data for selected event ID
Add time stamp to title	Select whether to include the time of the report in the report title. By default, the time is not included.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Generate event on success?	Select whether to raise an event when the report is successfully generated. By default, events are enabled.
Severity level for report success	Specify a severity level for the event raised when the report is generated successfully. Default is 35.
Severity level for report with no data	Specify a severity level for the event raised when no data for the report is found within the selected time interval. Default is 25.
Severity level for report failure	Specify a severity level for the event raised when report generation fails. Default is 5.

TracerouteException Report Details

The following topics explain the different sections of the report output.

Exception Traceroute

This section summarizes an "exception traceroute," a traceroute test run automatically when a threshold was crossed. The exception traceroute reported on is the one associated with the event whose ID was specified in the report script parameters.

The table includes the source and target locations of the exception traceroute, the time the traceroute was run, the route ID of the traceroute, the number of hops in the traceroute, the total latency of the traceroute, the Knowledge Script that raised the associated event, the ID of the job that raised the associated event, the ID of the associated event, the message of the associated event, and the time of the first occurrence of the associated event.

The route ID of the exception traceroute refers to the route ID associated with the routes listed in the "Route Frequency" and "Route Details" sections, described below.

Traceroute Analysis

This section compares the details of the exception traceroute that is the focus of this report against the details of the most common baseline traceroute.

The hop locations and latencies of the exception traceroute are listed side-by-side with the hop locations and latencies of the baseline traceroute. If a hop location is the same for both traceroutes based on the IP addresses of the hops, the hop location is listed in the column of common hops.

The most common baseline traceroute is determined using the following steps:

1. Find the traceroute with the highest baseline frequency.
2. If more than one traceroute shares the highest baseline frequency, select the traceroute that has the same route ID as the exception traceroute. Or else select the traceroute that has the lowest exception frequency.
3. If multiple traceroutes share the highest baseline frequency and the lowest exception frequency, choose the traceroute with the lowest route ID.

Note
If no baseline data is available, the table is not created.

Route Frequency

This section summarizes all of the distinct routes from the source location to the target location seen during the time period of the report. When comparing routes, two routes are considered to be the same if all of the following conditions are met:

1. The source location names are identical.
2. The target location names are identical.
3. The number of hops for both routes are identical.
4. The IP addresses at each hop are identical. The hop names are not considered.

For each distinct route, the table lists its route ID, the frequency of the route when collected using the Networks-RT_Traceroute Knowledge Script (Baseline Route Frequency), the average latency of this route when collected using the Networks-RT_Traceroute Knowledge Script (Average Baseline Route Latency), the frequency of the route when collected using either traceroute Action Knowledge Script (Exception Route Frequency), and the average latency of this route when collected using either traceroute Action Knowledge Script (Average Exception Route Latency).

If no data has been collected using the Networks-RT_Traceroute Knowledge Script for a route, the route has a Baseline Route Frequency of 0.00%, and the Average Baseline Route Latency is blank. Likewise, if no data has been collected using either traceroute Action Knowledge Script for a route, the route has an Exception Route Frequency of 0.00%, and the Average Exception Route Latency is blank.

Note
The route ID for each route is not guaranteed to be constant between reports with different time periods for a given source and target pair. The route IDs are determined at the time the report is generated, and are dependent on the data points included in the report. For example, you may have collected data points for three distinct routes between source “A” and target “E” like the following:

- A - B - C - D - E
- A - F - G - H - E
- A - X - Y - Z - E

If the time period for the report covers all of these data points, the report may list the "A-B-C-D-E" route with Route ID = 1, the "A-F-G-H-E" route with Route ID = 2, and the "A-X-Y-Z-E" route with Route ID = 3. However, if the time period of the report is changed to exclude the "A-B-C-D-E" data points, then the Route ID values for the remaining routes are shifted up by 1 - the "A-F-G-H-E" route will have Route ID = 1, and the "A-X-Y-Z-E" route will have Route ID = 2.

Route Details

This section provides details for each of the distinct routes from the source location to the target location seen during the time period of the report. A separate table is created for each distinct route.

Each table lists the hops for a particular route, with one hop per table row. For each hop, the row contains the average latency for the hop when collected using the Networks-RT_Traceroute Knowledge Script (Average Baseline Hop Latency), the average latency for the hop when collected using either traceroute Action Knowledge Script (Average Exception Hop Latency), the IP address for the hop (Address), and the resolved name for the hop (Name).

Similar to the Route Frequency table, if no data has been collected using the Networks-RT_Traceroute Knowledge Script for a route, the Average Baseline Hop Latency is blank for each hop. Likewise, if no data has been collected using either traceroute Action Knowledge Script for a route, the Average Exception Hop Latency is blank for each hop. And if an individual hop could not be determined, the Average Baseline Hop Latency and Average Exception Hop Latency is "0.000", the Address is "0.0.0.0", and the Name is blank.

Last 10 Exception Routes

This section provides details for up to ten exception traceroutes from the source location to the target location seen during the time period of the report. If fewer than 10 exception traceroutes are collected during the time period of the report, only those traceroutes are included. If more than 10 exception traceroutes are collected during the time period of the report, the report selects the ten most recent exception traceroutes. A separate table is created for each exception traceroute.

The data in the exception traceroute tables is similar to that in the Route Details tables. However, the data in the exception traceroute tables is the raw data for only one particular traceroute instance. The latency values in the exception traceroute tables are not averaged against other traceroute instances.

Parameters

This section provides details about the creation of the report itself. The table lists the ID of the event associated with the exception traceroute used as the basis of the report, the description of the report, and the time the report was created.

Report_TracerouteProfile

Use this Report Knowledge Script to generate a report that summarizes the averaged traceroute statistics for a given source and target location combination, along with the last 10 exception traceroutes for the pair.

Specify any time range from which to include data for the report; the default is 14 days before the time the report is created.

Resource Object

Report Agent (with Networks-RT subfolder)

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Traceroute source location	Select an AppManager ResponseTime for Networks node, the node from which the traceroute was run. Do not leave blank. Specify only one source.
Traceroute target location	Select an AppManager ResponseTime for Networks node, some other AppManager node, an IP address, or a URL to which the traceroute was run. Do not leave blank. The report validates whether traceroute data is associated with the source-target pair and reports an error if none is. Specify only one target.
Select time range	Specify the time period whose baseline and exception data should be included. Default includes all data from the previous 14 days up to the current time.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter card?	Select whether to include a table of report parameters at the end of the report. By default, the table is included.
Include route frequency table?	Select whether to include table of route frequencies in the report. By default, the table is included.
Include route details table?	Select whether to include route details table(s) in the report. By default, the table is included.
Include last 10 exception route tables?	Select whether to include last 10 exception route table(s) in the report. By default, the table is included.
Select output folder	Select a report filename and folder. Default is "`Networks-RT_TracerouteProfile\default.htm`".
Add job ID to output folder name?	Select whether to append the report job ID to the report output folder name. By default, the job ID is not appended.

Index-Report Title	Choose report title, author, company, component, description, expiration period, and custom fields. Defaults are: Title = Networks-RT Traceroute Profile Author = NetIQ AppManager Company = Your company here Component = NetIQ AppManager 5.0 Networks-RT Module Description = Reports for Networks-RT: Traceroute Profile Expiration Period = Expires after 7 days Custom Field 1 = Networks-RT Endpoint, Traceroute Profile Custom Field 2 = Baseline and exception traceroute data for selected source and target locations.
Add time stamp to title	Select whether to include the time of the report in the report title. By default, the time is not included.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events
Generate event on success?	Select whether to raise an event when the report is successfully generated. By default, events are enabled.
Severity level for report success	Specify a severity level, from 1 to 40, to indicate the importance of the successful report generation event. Default is 35.
Severity level for report with no data	Specify a severity level, from 1 to 40, to indicate the importance of the event when no data for the report is found within the selected time interval. Default is 25.
Severity level for report failure	Specify a severity level, from 1 to 40, to indicate the importance of the event when report generation fails. Default is 5.

TracerouteProfile Report Details

The Traceroute report output contains several different sections:

Traceroute

This section lists the traceroute source and target locations specified in the report script parameters.

Route Frequency

This section summarizes all of the distinct routes from the source location to the target location seen during the time period of the report. When comparing routes, two routes are considered to be the same if all of the following conditions are met:

1. The source location names are identical.
2. The target location names are identical.
3. The number of hops for both routes are identical.
4. The IP addresses at each hop are identical. Hop names are not considered.

For each distinct route, the table lists its route ID, the frequency of the route when collected using the Networks-RT_Traceroute Knowledge Script (Baseline Route Frequency), the average latency of this route when collected using the Networks-RT_Traceroute Knowledge Script (Average Baseline Route Latency), the frequency of the route when collected using either traceroute Action Knowledge Script (Exception Route Frequency), and the average latency of this route when collected using either traceroute Action Knowledge Script (Average Exception Route Latency).

If no data has been collected using the Networks-RT_Traceroute Knowledge Script for a route, the route has a Baseline Route Frequency of 0.00%, and the Average Baseline Route Latency is blank. Likewise, if no data has been collected using either traceroute Action Knowledge Script for a route, the route has an Exception Route Frequency of 0.00%, and the Average Exception Route Latency is blank.

Note

The route ID for each route is not guaranteed to be constant between reports with different time periods for a given source and target pair. The route IDs are determined at the time the report is generated and are dependent on the data points included in the report. For example, you may have collected data points for three distinct routes between source "A" and target "E" like the following:

- A - B - C - D - E
- A - F - G - H - E
- A - X - Y - Z - E

If the time period for the report covers all of these data points, the report may list the "A-B-C-D-E" route with Route ID = 1, the "A-F-G-H-E" route with Route ID = 2, and the "A-X-Y-Z-E" route with Route ID = 3. However, if the time period of the report is changed to exclude the "A-B-C-D-E" data points, the Route ID values for the remaining routes are shifted up by 1, the "A-F-G-H-E" route has Route ID = 1, and the "A-X-Y-Z-E" route has Route ID = 2.

Route Details

This section provides details for each of the distinct routes from the source location to the target location seen during the time period of the report. A separate table is created for each distinct route.

Each table lists the hops for a particular route, with one hop per table row. For each hop, the row contains the average latency for the hop when collected using the Networks-RT_Traceroute Knowledge Script (Average Baseline Hop Latency), the average latency for the hop when collected using either traceroute Action Knowledge Script (Average Exception Hop Latency), the IP address for the hop (Address), and the resolved name for the hop (Name).

Similar to the Route Frequency table, if no data has been collected using the Networks-RT_Traceroute Knowledge Script for a route, the Average Baseline Hop Latency is blank for each hop. Likewise, if no data has been collected using either traceroute Action Knowledge Script for a route, the Average Exception Hop Latency is blank for each hop. And if an individual hop could not be determined, the Average Baseline Hop Latency and Average Exception Hop Latency is "0.000", the Address is "0.0.0.0", and the Name is blank.

Last 10 Exception Routes

This section provides details for up to 10 exception traceroutes from the source location to the target location seen during the time period of the report. If fewer than 10 exception traceroutes were collected during the time period of the report, only those traceroutes are included. If more than ten exception traceroutes were collected during the time period of the report, the report selects the 10 most recent exception traceroutes. A separate table is created for each exception traceroute.

The data in the exception traceroute tables is similar to that in the Route Details tables. However, the data in the exception traceroute tables is the raw data for only one particular traceroute instance. The latency values in the exception traceroute tables are not averaged against other traceroute instances.

Parameters

This section provides details about the creation of the report itself. The table lists the source and target locations as specified in the report script parameters, the start time and end time between which to include traceroute data as specified in the report script parameters, a description of the report, and the time it was created.

Net-RT-Import_KSGenerator

These Knowledge Scripts are created using the KSGenerator. They are accessed via the **Net-RT-Import** tab in the AppManager Console.

Note
Context-sensitive Help is not available for imported Knowledge Scripts. To access Help for Net-RT-Import scripts, launch the online Help for AppManager. In the left pane or Table of Contents of the Help window, click Knowledge Script Reference, then Networks-RT Knowledge Scripts. Scroll through the table shown in the right pane and click Net-RT-Import_KSGenerator to view Help for these scripts.

Resource Object

Networks-RT

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

The following table describes many of the common parameters found in imported Knowledge Scripts. Not all parameters are available in every script.

Parameter	How to Set It
How many timing records to generate	An endpoint creates a timing record each time it goes through this loop. Many scripts have two loops: the outer loop controls the number of timing records, while the inner loop controls the number of transactions per timing record. By adjusting the inner loop, you can run large scripts without ending up with too many timing records. Defaults to 1, and is marked as a Hidden Parameter in the KSGenerator. NetIQ Corporation recommends to set this value to 1.
Transactions per timing record	Many scripts have two loops controlled by `LOOP` commands: the outer loop controls the number of timing records, while the inner loop controls the number of transactions per timing record. By adjusting the inner loop, you can run large scripts without generating too many timing records. This variable controls the number of transactions performed per timing record. A setting of "1" equates to one timing record per transaction. While this setting yields the most granular results, revealing variations in performance metrics, it also tends to create a huge number of timing records. Larger values lets you run long tests that generate fewer timing records. Because endpoints return a timing record for each collection of transactions in this loop, results are averaged, which may hide variations in network response. The best values for this variable make the script loop enough times to generate a timing record about once a second. The proper setting requires a bit of trial and error, and depends on the speed of the network and the type of transaction.
How many bytes of data in each SEND	The `SEND` command has four variables: • how many bytes to send • what size buffers to use on each `SEND` • what type of data to send • the rate at which to send the data For example, if you chose "`SEND 1000, 100, ZEROS, UNLIMITED`," an endpoint would send 1000 bytes, 100 bytes at a time, with all zeros as data, as fast as possible. This `SEND` command would result in 10 `Send` calls to the communications API. Some scripts use the same variable for the send size and the buffer size. This was designed so that the data is always sent in one block. Send and receive buffers can be set to the value "`DEFAULT`." This tells the endpoint to use buffers that are the default size for the network protocol being used. `DEFAULT` lets you use the default buffer size for each protocol, without having to modify the script to handle protocol differences. The default value is different depending on the protocol and platform being used. An endpoint uses the common value for its particular environment. To have the endpoint send data of varying packet sizes, use one of the random distributions: Uniform, Normal, Poisson, or Exponential. For more information, see the **Note** below.

Parameter	How to Set It
How many bytes of data in each RECEIVE	The RECEIVE command has two variables: • how many bytes to receive • what size buffers to use on each RECEIVE. For example, if you chose "RECEIVE 1000, 100," an endpoint would receive 1000 bytes, 100 bytes at a time. This RECEIVE command would result in 10 calls to the communications API. Some scripts use the same variable for the receive size and the buffer size. This was designed so that all of the data is received in one block. Send and receive buffers can be set to the value "DEFAULT." This tells the endpoint to use buffers that are the default size for the network protocol being used. DEFAULT lets you use the default buffer size for each protocol, without having to modify the script to handle protocol differences. The default value is different depending on the protocol and platform being used. An endpoint uses the most common value for its particular environment. To have the endpoint send data of varying packet sizes, use one of the random distributions: Uniform, Normal, Poisson, or Exponential.
Amount of data to be sent	The SEND command has four variables: • how many bytes to send • what size buffers to use on each SEND • what type of data to send • the rate at which to send the data. For example, if you chose "SEND 1000, 100, ZEROS, UNLIMITED," an endpoint would send 1000 bytes, 100 bytes at a time, with all zeros as data, as fast as possible. This SEND command would result in 10 Send calls to the communications API.
How many bytes in the transferred file	The SEND command has four variables: • how many bytes to send • what size buffers to use on each SEND • what type of data to send • the rate at which to send the data. For example, if you chose "SEND 1000, 100, ZEROS, UNLIMITED," an endpoint would send 1000 bytes, 100 bytes at a time, with all zeros as data, as fast as possible. This SEND command would result in 10 Send calls to the communications API. In the file transfer scripts, you can set the size of the simulated file to be sent. Remember that an endpoint is sending this amount of data, but it is not doing any file I/O.
Milliseconds to wait before responding	This variable lets you simulate a user delay or processing at the endpoint. Before the next script command is executed, the endpoint sleeps for the number of milliseconds specified here. The SLEEP does not consume CPU cycles, so it is only simulating the delay, not the CPU or other overhead of a real application or user. Endpoints can sleep the same amount every time, or for a random period of time if you select one of the random distributions: Uniform, Normal, Poisson, or Exponential. A Constant value of 1000 causes an endpoint to sleep for 1 second. For a Uniform distribution, enter the range for the random sleep time. For example, if you want the endpoint to sleep for somewhere between 2 and 5 seconds, enter 2000 for the Lower limit value and 5000 for the Upper limit. By default the delay is set to a Constant value of 0, which means that an endpoint immediately begins executing the script commands.

Parameter	How to Set It
Milliseconds to pause	Control how frequently transactions are executed. Set the number of milliseconds to sleep before starting to execute more commands. Normally used to simulate an end user running a transaction on a regular basis, for example, once per second. A value of 1000 will cause an endpoint to sleep for one second. By default the delay is set to 0, which means that an endpoint executes the scripts as quickly as possible.
What type of data to send	This variable lets you control the contents of the data sent during a test. The default, NOCOMPRESS, defeats most network compression algorithms by sending a loop of randomly generated data. ZEROS sends all zero data. The standard text file NEWS.CMP and the standard graphics file LENA.CMP should be used for most cases where text data or graphics data is required. Data types ZEROS and NOCOMPRESS are internally generated and therefore don't require any external files. All others require that the corresponding .CMP files be installed on the endpoints, and are loaded during test initialization. Only the standard data types, NEWS.CMP, LENA.CMP, and TRANS.CMP are installed by default.
Pause before the first transaction	Simulates a user delay or processing at the client side. Before the first script command is executed, Endpoint 1 sleeps for the number of milliseconds specified here. A SLEEP does not consume CPU cycles, so it only simulates a delay, not the CPU or other overhead of a real application or user. The longest allowable time for initial_delay is 90 minutes, or 5400000 milliseconds. Longer values cause Endpoint 2 to time out, and the connection to fail. Endpoints can sleep the same amount every time, or for a random period of time if you select one of the random distributions: Uniform, Normal, Poisson, or Exponential. A Constant value of 1000 causes an endpoint to sleep for one second. For any of the distributions, enter a range for the random sleep time. For example, if you want the endpoints to sleep for somewhere between 2 and 5 seconds, enter 2000 for the Lower limit value and 5000 for the Upper limit. By default the delay is set to a Constant value of 0, which means that an endpoint immediately begins executing the script commands.
Pause before answering	Simulates a user delay or processing at the client side. Before the next script command is executed, Endpoint 1 sleeps for the number of milliseconds specified. The SLEEP does not consume CPU cycles, so it only simulates a delay, not the CPU or other overhead of a real application or user. Endpoints can sleep the same amount every time, or for a random period of time if you select one of the random distributions: Uniform, Normal, Poisson, or Exponential. A Constant value of 1000 causes an endpoint to sleep for one second. For any of the four distributions, enter a range for the random sleep time. For example, if you want the endpoints to sleep for somewhere between 2 and 5 seconds, enter 2000 for the Lower limit value and 5000 for the Upper limit. By default the delay is set to a Constant value of 0, which means that an endpoint immediately begins executing the script commands.
What type of control data to send	This variable lets you control the contents of the control data sent by some scripts. The standard text file NEWS.CMP is used, to simulate the transfer of text information like file and directory names. Data types ZEROS and NOCOMPRESS are internally generated and therefore don't require any external files. All others require that the corresponding .CMP files be installed on the endpoints, and are loaded during test initialization. Only the standard data types, NEWS.CMP, LENA.CMP, and TRANS.CMP are installed by default.

Parameter	How to Set It
How many bytes in server RECEIVEs	The RECEIVE command issued by the server has two variables: • how many bytes to receive • what size buffers to use on each RECEIVE For example, if you choose "RECEIVE 1000, 100," an endpoint receives 1000 bytes, 100 bytes at a time. This RECEIVE command would result in 10 calls to the communications API. This script variable emulates the buffer size commonly used in server applications. Some scripts use the same variable for the receive size and the buffer size; they are designed so that all data is received in one block. Send and receive buffers can be set to the value "DEFAULT." This tells an endpoint to use buffers that are the default size for the network protocol being used. DEFAULT lets you use the default buffer size for each protocol, without having to modify the script to handle protocol differences. The default value is different depending on the protocol and platform being used. An endpoint uses the most common value for its particular environment.
How many times to repeat the script	Some test scripts have three LOOPs. This outer loop repeats the entire sequence of flows, including the setup and takedown flows, which are not within the timing loops. The next loop controls the number of timing records created; the inner loop controls the number of transactions per timing record. By adjusting these three loops, you can run large test scripts without creating excessive test overhead. This variable controls the number of repetitions of the entire set of flows. Setting it to "1" causes this scripts to spend most of its time on the two inner loops--where the timing records and transactions are counted. Only set this value greater than its default of 1 when you're using this script for stress-testing--never for true performance measurements. The untimed traffic outside the timing loops can give you misleading throughput numbers.
Buffer size for control flows	The SEND and RECEIVE commands have variables that let you tailor the size of the buffers they use for sending and receiving, respectively. The variables determine the size of the buffer used for sending or receiving control flows. Send and receive buffers can be set to the value "DEFAULT." This tells an endpoint to use buffers that are the default size for the network protocol being used. DEFAULT lets you use the default buffer size for each protocol, without having to modify the script to handle protocol differences. The default value is different depending on the protocol and platform being used. An endpoint uses the most common value for its particular environment.
How many bytes are in the control flows	You can set the size of the file control information to be sent and received, in preparation for transferring the file. In a real file transfer, this usually consists of directory and filename information.
How many bytes are in the login flows	Set the size of the login information to be sent and received, in preparation for transferring the file. In a real file transfer, this usually consists of user ID and password information. This value is typically 15 to 30 bytes.

Parameter	How to Set It
What port to use for Endpoint 2	You can specify the destination port number to use when setting up the connection between the endpoints, or you can let it be automatically assigned. Select AUTO to let it be assigned automatically; this gives the best performance. Clear AUTO and enter a port number between 1 and 65535 if you are trying to emulate a specific application. This capability is useful when testing devices that filter traffic based on their port number, such as firewalls. Use AUTO if possible when testing with multiple pairs. If the same port is specified for multiple pairs, the performance degrades, since the pairs must share/serialize the use of the port to run the test. Here are the categories of port numbers: • 1-1023: reserved for well-known services such as FTP • 1024: reserved by IANA • 1025 - 5000: typical range for user-defined services • 5000 - 65535: typical range for server software
How many bytes in the server info	Set the size of the server ID message to be sent and received, in preparation for transferring news articles. This value is typically 15 to 30 bytes.
How many bytes in the header	Set the size of the article header to be sent and received, in preparation for transferring news articles.
How many bytes in the article	Set the size of the article to be sent and received, in preparation for transferring news articles.
Number of groups	Set the number of groups to be retrieved.
Number of articles	Set the number of articles to be retrieved.
Pause between groups	This variable lets you simulate a user delay or processing the between groups. Before the next script command is executed, the endpoint sleeps for the number of milliseconds specified. The SLEEP does not consume CPU cycles, so it is only simulating the delay, not the CPU or other overhead of a real application or user. Endpoints can sleep the same amount every time, or for a random time period by choosing one of the distributions. A Constant value of 1000 causes an endpoint to sleep for one second. For a Uniform distribution, enter the range for the random sleep time. For example, if you want the endpoints to sleep for somewhere between 2 and 5 seconds, enter 2000 for the Lower limit value and 5000 for the Upper limit value. By default the delay is set to a Constant value of 0, which means that an endpoint immediately begins executing the script commands.
Pause between articles	Simulates a user delay or processing the between articles. Before the next script command is executed, the endpoint sleeps for the number of milliseconds specified here. The SLEEP does not consume CPU cycles, so it is only simulating the delay, not the CPU or other overhead of a real application or user. Endpoints can sleep the same amount every time, or for a random period if you choose one of the random distributions. A Constant value of 1000 causes an endpoint to sleep for one second. For a Uniform distribution, enter the range for the random sleep time. For example, if you want to sleep for somewhere between 2 and 5 seconds, enter 2000 for the Lower limit value and 5000 for the Upper limit. By default the delay is set to a Constant value of 0, which means that an endpoint immediately begins executing the script commands.

Parameter	How to Set It
How fast to send data	This variable controls the rate at which data is sent. To send data at a certain speed, enter the rate value and units. To send data as fast as possible, select `UNLIMITED`. Or select common data rates. The format for common data rates must include a numeric value and the data rate units. For example: • 28.8 kbps (kilobits (1,000) per second) • 1420 KBps (kilobytes (1,024) per second) • 1.544 Mbps (megabits (1,000,000) per second) Valid units are: • kbps: 1,000 bits per second • kBps: 1,000 bytes per second • Kbps: 1,024 bits per second • KBps: 1,024 bytes per second • Mbps: 1,000,000 bits per second • Gbps: 1,000,000,000 bits per second
How connections are terminated	Determines whether `TCP DISCONNECT` commands in application scripts are abortive or normal. By default, NetIQ application scripts use an abortive close, with a `RST` flag, which closes the connection immediately. Change the `close_type` to normal to use a `FIN` flag to close the connection slowly, with acknowledgments from the receiving computer. With an abortive close, the protocol stack on the receiving endpoint cannot reclaim network resources taken by the connection if the `RST` is lost, and may linger indefinitely in `FIN_WAIT` state. The normal close specifies that if the `FIN` is lost, the endpoints remain in `TIME_WAIT` state only until the stack's timeout period elapses. Valid for TCP only.
What port to use for Endpoint 1	You can specify the source port number to use when setting up the connection between the endpoints, or you can let it be automatically assigned. Select `AUTO` to let it be assigned automatically; this gives the best performance. Clear `AUTO` and enter a port number from 1 to 65535 to emulate a specific application. This capability is useful when testing devices that filter traffic based on their port number, such as firewalls. Use `AUTO` if possible when testing with multiple pairs. If the same port is specified for multiple pairs, performance degrades because the pairs must share/serialize the use of the port to run the test. Here are the categories of port numbers: • 1-1023: reserved for well-known services such as FTP • 1024: reserved by IANA • 1025 - 5000: typical range for user-defined services • 5000 - 65535: typical range for server software

Note

Four types of random mathematical distributions can be used for values in certain parameters, such as delay parameters:

- **Uniform**

  The distribution between the upper and lower limit is completely uniform. Any number within the upper and lower limits is as likely to be used as any other number.

- **Normal**

The Marsaglia-Bray algorithm is used to generate the normal distribution. The average value of the distribution is determined from the upper and lower limit. In a normal distribution, most values occur within +/-3 standard deviations with respect to the average. The standard deviation is also calculated from the upper and lower limits, as no value exceeds those limits.

- **Poisson**

  This distribution is calculated as follows:

  ```
  standard deviation=(high-low)/6
  mean=standard deviation**2
  ```

  The random number generator only returns the numbers in the given low/high range, effectively truncating the distribution curve at the ends.

- **Exponential**

  This distribution is calculated as follows:

  ```
  mean=[(low + high)/2]- low
  a= 1/mean
  variance= 1/(a**2)
  standard deviation= 1/a
  standard deviation=mean
  ```

  The random number generator generates numbers between 0 and (high-low), and increments each number by low to ensure no number is less than low effectively shifting the distribution curve to the right.

Chapter 48
NortelBCM Knowledge Scripts

The NortelBCM category provides the following Knowledge Scripts for monitoring Nortel Business Communications Manager (Nortel BCM) resources.

From the Knowledge Script view of Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
BCM_HealthCheck	Monitors the operational (up or down) status of Nortel BCM services.
BCM_QoSInterfaceActivity	Monitors the number of dropped packets for LAN and WAN links.
BCM_QoSLog	Monitors the MOS for the following codecs: G.711a, G.711u, G.723 (5.3 kpbs), G.723 (6.3 kpbs), and G.729.
BCM_QoSPrioritySessions	Monitors the number of priority sessions for LAN and WAN links. Priority sessions are those that request the use of the PREMIUM queue 1.
BCM_QoSQueueUsage	Monitors the number of dropped packets for the queues of LAN and WAN links.
BCM_SystemUsage	Monitors total CPU, CPU interrupt handling time, physical memory usage, and memory pages per second.
Report_ServicesAvailability	Summarizes the availability of Nortel BCM services. This report uses the data collected by the BCM_HealthCheck script.
Report_SystemUsage	Summarizes the average Nortel BCM CPU and physical memory usage. This script uses the data collected by the BCM_SystemUsage script.
Sys_AsciiLog	Scans an ASCII text file for specific strings and messages logged since the last monitoring interval.
Sys_CpuByProcess	Monitors whether specific processes have exceeded CPU thresholds.
Sys_CpuLoaded	Monitors both CPU usage and the queue length.
Sys_DNSConnectivity	Checks the connectivity between a computer and its DNS server.
Sys_EventLog	Monitors and filters information in the Event Log based on criteria that you specify.
Sys_FailedLogon	Monitors failed logon attempts to the server since the last interval.
Sys_FileChanged	Compares the size, timestamp, and attributes of a specified file from one interval to the next.
Sys_FilesCompare	Compares the size, timestamp, and attributes of two files.

Knowledge Script	What It Does
Sys_GeneralCounter	Monitors any user-specified Performance Monitor counter. This script differs from Sys_IntervalCounter in that it takes a "snapshot" of a counter when you run the script; IntervalCounter monitors the change in a counter between one run of the script and the next.
Sys_IntervalCounter	Monitors the change in any user-specified counter. This script differs from Sys_GeneralCounter in that it monitors the change in a counter between one run of the script and the next; GeneralCounter takes a "snapshot" of a counter when you run the script.
Sys_LogicalDiskSpace	Monitors logical disk space usage.
Sys_MemUtil	Monitors the usage of physical memory, virtual memory, and paging files.
Sys_PagingHigh	Monitors pagefile reads/writes per second.
Sys_ProcessDown	Determines whether specified processes are running.
Sys_Processes	Monitors the number of current processes.
Sys_ServiceChange	Monitors any changes to user-specified services.
Sys_ServiceDown	Checks whether any user-specified service is down.
Sys_ServiceHung	Detects whether a specified service is hung.
Sys_SystemUpTime	Monitors the number of hours that a system has been operational since its last reboot.
Sys_TopCpuProcs	Monitors the CPU usage of all processes and identifies the top consumers.
Sys_TopMemoryProcs	Monitors the memory usage of all processes and identifies the top consumers.

BCM_HealthCheck

Use this Knowledge Script to monitor the operational (up or down) status of Nortel BCM services. This script records a value of 1 if a service is running and a value of 0 if a service is not running. A service is considered non-running if its status is one of the following:

- Start pending
- Stop pending
- Paused
- Stopped
- Continue pending
- Pause pending

This script raises an informational event if it finds a disabled service.

To make the most of the data gathered by this script, run Report_ServicesAvailability.

Note
For more information about BCM services, see the Nortel Business Communications Manager 3.6. Management Guide.

Resource Object

NortelBCM object

Default Schedule

The default schedule is **Every minute**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Set to **y** to collect data for reports and graphs. The default is y.

Parameter	How To Set It
Event severity if service is not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which a service is not running. Set to **0** if you do not want to raise events. The default is 5.
Monitor [...]?	Set to **y** to monitor the following services. The default is y for each. • Call Detail Recording • Media Gateway Server • Media Services Manager • Multi Dialup Manager • Net Link Manager • Protected Storage • Routing and Remote Access • UNISTIM Terminal Proxy Server • Voice CFS • Voice CTI • Voice Licensing • Voice MSC • Voice Watchdog

BCM_QoSInterfaceActivity

Use this Knowledge Script to monitor the number of dropped packets for LAN and WAN links. This script raises an event if the percentage of dropped packets exceeds the threshold you set. In addition, this script generates data streams for the number of total packets, the number of priority packets, the number of best-effort packets, and the number of dropped packets.

Resource Object

NortelBCM object

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the percentage of dropped packets exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about packets for reports and graphs. The default is n.
Link to monitor	Select the link that you want to monitor. Choose from Dial-up, LAN 1, LAN2, UTWAN, WAN1, and WAN2. The default is LAN 1.
Threshold - Maximum dropped packets	Set the threshold for the highest percentage of dropped packets that can occur before an event is raised. The default is 10%.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of dropped packets exceeds the threshold. The default is 5.

BCM_QoSLog

If you use VoIP trunking, use this Knowledge Script to monitor the MOS for the following codecs in transmit and receive directions: G.711a, G.711u, G.723-5.3 kbps, G.723-6.3 kbps, and G.729. This script raises an event for every line in the Nortel QoS Monitor log that contains a MOS that exceeds a threshold. Entries in the QoS Monitor log to the same destination remote gateway are averaged to a single data point.

Because duplicate events are collapsed into one by default, you can view only the most recent event for a monitored remote gateway. You can turn off event collapsing if you want to see all of the events for a monitored remote gateway. Before you run the script, click to uncheck the following option on the **Advanced** tab of the Properties dialog box: **Collapse duplicate events into a single event**.

Note
Enable the QoS Monitor on the BCM before you run this script. For information about enabling the QoS monitor, see the Programming Operations Guide for Nortel Business Communications Manager 3.6.

Resource Object

NortelBCM object

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the MOS threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about MOS for reports and graphs. Entries in the QoS log to the same destination remote gateway are averaged to a single data point per script iteration. The default is y.
Threshold - Minimum acceptable MOS	Set the threshold for the lowest MOS that can occur before an event is raised. The default is 3.60.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS score fails to meet the minimum threshold. The default is 5.
Monitor [...]?	Set to **y** to monitor the following codecs. The default is y. • G.711a • G.711u • G.723-5.3 kbps • G.723-6.3 kbps • G.729
Destination gateway to filter	Type the name or IP address of the target remote gateway. Use commas to separate multiple names or IP addresses.

BCM_QoSPrioritySessions

Use this Knowledge Script to monitor the number of priority sessions for LAN and WAN links. Priority sessions are those that request the use of Premium queue 1. This script raises an event if the number of sessions not served exceeds the threshold that you set. In addition, this script generates data streams for the number of requested priority sessions and the number of priority sessions that are not served.

Note
For more information about using queues and priority sessions to support IP service classes, see the "Policy-enabled Networking" chapter in the Programming Operations Guide for Nortel Business Communications Manager 3.6.

Resource Object

NortelBCM object

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about requested and not-served priority sessions, for reports and graphs. The default is n.
Link to monitor	Select the link that you want to monitor. Choose from Dial-up, LAN 1, LAN2, UTWAN, WAN1, and WAN2. The default is LAN 1.
Threshold - Maximum sessions not served	Set the threshold for the most sessions that can be "not served" before an event is raised. The default is 4 sessions.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 5.

BCM_QoSQueueUsage

Use this Knowledge Script to monitor the number of dropped packets for the queues for LAN and WAN links. This script raises an event if the number of dropped packets exceeds the threshold you set. In addition, this script generates data streams for the number of total packets and dropped packets for queues 1 through 8.

Service class behaviors are implemented using a scheduler and queues 1 through 8. Queue 1 has the highest priority, referred to as Strict Priority. Queues 2 to 8 are scheduled according to a Weighted Fair Queuing (WFQ) scheme. The following table summarizes the mappings between service classes, queues, and DSCP codes.

Service Class	Default DSCP	BCM Queue	BCM Scheduler
Premium	40, 46	1	Strict Priority
Network	48, 56	2	Weighted Fair Queuing
Platinum	34, 36, 38	3	Weighted Fair Queuing
Gold	26, 28, 30	4	Weighted Fair Queuing
Silver	18, 20, 22	5	Weighted Fair Queuing
Bronze	10, 12, 14	6	Weighted Fair Queuing
Standard	0	7	Weighted Fair Queuing
Standby	2	8	Weighted Fair Queuing

Note
For more information about using queues and priority sessions to support IP service classes, see the "Policy-enabled Networking" chapter in the Programming Operations Guide for Nortel Business Communications Manager 3.6.

Resource Object

NortelBCM object

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of dropped packets exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about packets for reports and graphs. The default is n.
Link to monitor	Select the link that you want to monitor. Choose from Dial-up, LAN 1, LAN2, UTWAN, WAN1, and WAN2. The default is LAN 1.

Parameter	How To Set It
Threshold - Maximum dropped packets	Specify the highest number of packets that can be dropped before an event is raised. The default is 10 packets.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of dropped packets exceeds the threshold. The default is 5.

BCM_SystemUsage

Use this Knowledge Script to monitor total BCM CPU, CPU interrupt handling time, physical memory usage, and memory pages per second. This script raises an event if any threshold is exceeded. In addition, this script data streams for percentage of CPU, percentage of CPU interrupt handling time, physical memory usage, and memory pages per second.

Resource Object

NortelBCM object

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is y.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 10.
Threshold - Maximum system CPU usage	Specify the maximum percentage of system CPU resources that can be in use before an event is raised. The default is 80%.
Threshold - Maximum system CPU interrupt handling time	Specify the maximum percentage of system CPU interrupt handling time that can be in use before an event is raised. The default is 25%.
Threshold - Maximum system memory usage	Specify the maximum percentage of system memory that can be in use before an event is raised. The default is 80%.
Threshold - Maximum system memory pages/second	Specify the maximum number of system memory pages per second that can be in use before an event is raised. The default is 10.

Report_ServicesAvailability

Use this Knowledge Script to summarize the availability of each Nortel BCM service, per server within a time range. This report uses the data collected by the BCM_HealthCheck script.

Resource Object

Report object

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data Source	
Select data wizard	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the Knowledge Scripts that collected the data that you want to include in the report. The default is BCM_HealthCheck.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Decimal accuracy for % values	Specify the number of decimal places that you want to see in the values displayed in this report. The default is 3.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties of the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is `NortelBCMServicesAvailability`.
Add job ID to output folder name?	Set to y to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set the report properties as desired, including a title for the report. The default title is Nortel BCM Services Availability.

Parameter	How To Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp consists of the date and time the report was generated. The default is n. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has not data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_SystemUsage

Use this Knowledge Script to summarize the average BCM CPU and physical memory usage within a specified time frame. This script uses the data collected by the BCM_SystemUsage script.

Resource Object

Report object

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data Source	
Select data wizard	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the Knowledge Scripts that collected the data that you want to include in the report. The default is BCM_SystemUsage.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Chart Settings	
Include CPU chart?	Set to **y** to include a chart that details CPU usage. The default is y.
Include CPU interrupt handling time chart?	Set to **y** to include a chart that details CPU interrupt handling time. The default is y.
Include physical memory chart?	Set to **y** to include a chart that details physical memory. The default is y.
Include memory pages/sec chart?	Set to **y** to include a chart that details memory pages per second. The default is y.
Chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Chart color scheme	Select a color scheme template. The default is NetIQ1.
Chart Thresholds	
Threshold - CPU usage	Specify the CPU usage threshold to display on charts in the report. The default is 0%.
Threshold - CPU interrupt handling time	Specify the CPU interrupt handling time threshold to display on the charts in the report. The default is 0%.
Threshold - Memory usage	Specify the physical memory threshold to display on the charts in the report. The default is 0 KB.
Threshold - Memory pages/second	Specify the memory pages per second threshold to display on charts in the report. The default is 0.
Report Settings	

Parameter	How To Set It
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is `NortelBCMSystemUsage`.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set the report properties as desired, including a title for the report. The default title is Nortel BCM System Usage.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp consists of the date and time the report was generated. The default is n. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35.
Event severity when report has no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report has not data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Sys_AsciiLog

Use this Knowledge Script to scan an ASCII text file for specific strings and messages that have been logged since the last monitoring interval. This script allows you to specify a pattern or search string to look for in the ASCII file and reports the matching entries found in the monitoring period. Therefore, the script checks for changes to the text file that match the string you enter; it does not re-scan the entire file at each interval.

Note
If the text string you want to find contains quote marks such as "login:failed", you must enter an additional set of quote marks around the text string: ""login:failed"".

In the first interval, the script reads the file and inserts a marker at the end of the file. Note that the script does not search for a specified search string during the first interval. In subsequent intervals, the script checks the file for changes that match the search string you specified. The script raises an event if the number of lines matching your search criteria exceeds the threshold you set.

Note
This script reports the number of matched lines with each run of the script. The detail message contains the text data. If the detail message is larger than 32 KB, the data is saved in a file on the managed computer (<NetIQ_Home>\log, for example, C:\netiq\bin\log) and the detail message contains only the truncated data. If you generate these log files, you should periodically remove the files when you are done with them.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about the number of lines containing matching strings. The default is n.
File name (full path)	Specify the full path to the file you want to monitor. For example, enter `C:\temp\backup.log`. UNC names are also supported (`\\ENG\appdev\mylog.txt`). The default is `C:\temp\test.txt` **Tip** You can only specify one file name for any job instance. To monitor multiple logs or files, create separate Knowledge Script jobs.
Case sensitive?	Set to **y** if you want the Knowledge Script to match case when checking for a match to the search string. The default is n.

Parameter	How To Set It
Literal match?	Set to **y** if you want the Knowledge Script to register a match only when there is an exact match to the search string. For example, if you set this parameter to **y** and enter `"NetIQ AppManager"` as the Find string, only lines containing "NetIQ AppManager" are considered a match. If you set this parameter to **n** with the same string, any line that contains "NetIQ," "AppManager," or "NetIQ AppManager" is considered a match. The default is n.
Find pattern	Type all or part of the string you want the Knowledge Script to check for in the specified file. To match everything, leave this field blank. The default is blank.
Threshold - Maximum matching lines	Specify the number of times the script should detect a match before raising an event. Accept the default of 0 to make the first instance exceed the threshold and raise an event.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 5.

Sys_CpuByProcess

Use this Knowledge Script to monitor whether specific processes have exceeded CPU thresholds. This script monitors CPU usage for each named process, as well as the total CPU usage for all named processes.

To determine CPU usage, the script checks the percentage of processor time that the threads for each process used to execute instructions.

If a process is not found, the script assumes that the process is not currently running, and reports zero as the CPU result.

Note
This script does not detect invalid process names. If you enter an invalid process name, the script assumes that the process is not running, and reports 0 as the CPU result.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Processes to monitor	Type the names of one or more processes that you want to monitor, separated by commas and no spaces. **Note** Do not append .exe to the process names.
Raise event for each process if threshold is exceeded?	Set to **y** to raise events for individual processes if the associated thresholds are exceeded. The default is y.
Threshold - Maximum CPU usage for each process	Specify the maximum amount of CPU usage that can occur for each process before an event is raised. The default is 60%.
Collect data for each process?	Set to **y** to collect data about CPU usage, for graphs and reports, for individual processes. The default is n.
Raise event for all processes if threshold is exceeded	Set to **y** to raise an event if the threshold for all processes is exceeded. The default is y.
Threshold - Maximum CPU usage for all processes	Specify the maximum amount of CPU usage that can occur for all processes before an event is raised. The default is 95%.
Collect data for all processes?	Set to **y** to collect data about CPU usage, for graphs and reports, for all processes you are monitoring. The default is n.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.

Sys_CpuLoaded

Use this Knowledge Script to monitor total CPU usage and queue length to determine whether the CPU is overloaded. This script raises an event if both the total CPU usage and CPU queue length thresholds are exceeded.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about CPU usage and queue length for graphs and reports. The default is n.
Monitor overall load?	Set to **y** to monitor the overall CPU load. One data stream for all the CPUs on a system. Set to **n** to monitor individual CPUs separately. Note that multiple data streams may be created. The default is n. **Note** For a single-CPU system, monitoring all CPUs produces the same results as monitoring an individual CPU.
Threshold - Maximum CPU usage	Specify the maximum amount of CPU usage, user plus kernel, that can occur before an event is raised. The default is 90%.
Threshold - Maximum CPU queue length	Specify a queue length threshold. CPU queue length indicates how many processes are ready to run. If queue length exceeds the threshold, an event is raised. The default is two. **Note** If you are only interested in monitoring CPU usage, you can set the queue length threshold to -1.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5.

Example of Using this Script

On a multi-processor system, the total CPU utilization is the average percentage of time that all the processors on the system are busy executing non-idle threads. For example:

- If all processors are always busy, total CPU utilization is 100%.
- If all processors are 50% busy, total CPU utilization is 50%.
- If 25% of the processors are busy and all processors use a single queue in which threads wait for processor cycle, total CPU utilization is 25%.

Sys_DNSConnectivity

Use this Knowledge Script to check connectivity between a managed computer and its DNS server. If the DNS server is not specified, information will be gathered from the local domain and the default DNS server. This script generates a data stream for DNS connectivity.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event for DNS connectivity?	Set to **y** to raise an informational event about DNS connectivity. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. If set to **y**, the script returns a value of 100 if the DNS lookup and connection to the DNS server is successful and a value of 0 if the connection is not made. The default is n.
Remote DNS host name	Type the name of the DNS server to which you want to check the connection. If you don't enter a host name, AppManager uses the default DNS server for the managed computer. The default is wns1.HOME.net.
DNS domain name	Type the name of the DNS domain for the specified DNS server. If you don't enter a domain name, AppManager uses the local domain for the managed computer. The default is HOME.net.
Event severity for DNS connectivity	Set the severity level, from 1 to 40, to indicate the importance of an informational event that details DNS connectivity information. The default is 8.

Sys_EventLog

Use this Knowledge Script to monitor and filter information in the Event Log. With this script you can track event log entries that match a filtering criteria. The script works on an incremental basis, that is, it does not fully rescan the event log each time it runs, and returns all matching event log entries in the event or data point detail message.

Only the most recent batch of events can be viewed in the data point detail message. For example, assume you set the script to scan all previous entries in the event log and list 10 matching entries in each event detail message and when the script runs, 30 entries match your filtering criteria. In this case, the script raises three child events for the interval and each child event contains 10 entries. The oldest matching entries in one child event batch, the second oldest in batch two, and the most recent in batch three. If this same job is collecting data and you view the data detail message for the interval, only the entries from the third child event (batch 3) are displayed.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
Raise event for log entries?	Set to **y** to raise an event when the log contains entries for which you have filtered. The default is y.
Collect data?	Set to **y** to collect data about log entries for charts and graphs. The default is n.
Separate data?	Set to **y** to separate events entries from different log files into different data streams. If set to **n**, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. The default is n. For example, if you are monitoring both the System and Application logs, you may want to set this parameter to **y** so that events in the System log are tracked separately from events in the Application log.
Log source	Type the name of the event log you want to monitor. You can specify multiple event logs, separated by commas. For example: `System,Application`. The default is Application.
Type: Error	Set to **y** to monitor for error events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is y.
Type: Warning	Set to **y** to monitor for warning events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is y.
Type: Information	Set to **y** to monitor for information events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is n.

Parameter	How To Set It
Type: Success Audit	Set to **y** to monitor for success audit events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is n.
Type: Failure Audit	Set to **y** to monitor for failure audit events. If you set to **n**, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for *Collect data?* The default is n.
Instructions for filters: To limit the types of entries that raise events and the type of data that is collected, specify a search string that filters the following fields in the event log. The search string can contain criteria used to include entries, exclude entries, or both.· • Separate include and exclude criteria with a colon (:). For example, `net:logon` • Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ` • If you are specifying only include criteria, the colon is not necessary. For example, `SQL` • If you are specifying only exclude criteria, begin the search string with a colon. For example, `:defragmentation,cleanup`	
Event source filter	Specify one or more event sources. Separate multiple entries with commas. For example: `NTDS KCC,NTDS General`
Event category filter	Specify one or more categories. Separate multiple entries with commas.
Event ID filter	Specify a single event ID or a range of event IDs. Separate multiple entries with commas. For example: `1094,1404-1463`
Event user filter	Specify one or more user names. Separate multiple entries with commas. For example: `Pat,Chris,Alex`
Computer filter	Specify one or more computer names. Separate multiple entries with commas. For example: `SHASTA,MARS`
Event description filter	Specify a detail description or keywords in the description. The text string can contain spaces, underscores, and periods. Separate multiple entries with commas. For example: `data loss during system failures,corrupt indices,Inter-Site Transport objects failed`
Maximum number of entries per event report	Specify the maximum number of Application log events that can be returned in each event report. For example, if you set this value to 30 and AppManager finds 67 Application log events, then three event reports are raised: two reports containing 30 events and one report containing seven events. The default is 30. The Message column on the **Events** tab in the Operator Console displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.
Event severity for log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event. You may want to adjust the severity depending on the types of events for which you are checking. The default is 8.

Examples of Using this Script

You can customize this Knowledge Script in many ways based on your requirements.

To detect security failures:

Properties and Parameters	How You Might Set Them
Schedule interval	On the **Schedule** tab, set the interval to once every 10 minutes because you want a small window for checking for this type of problem.
Raise event?	Set to **y** to raise an event if conditions are met.
Log source	Specify the Security log.
Type:Failure Audit	Set to **y** to monitor for failure audit events.
Severity	Set to 2 to indicate a serious event.
Action	In the **Action** field on the **Action** tab, select **Action_MapiMail**. With this setting, AppManager will notify you by email if any security failure events are detected.

To detect all problems with your SQL Server:

Properties and Parameters	How You Might Set Them
Schedule interval	On the **Schedule** tab, set the interval to once every 30 minutes.
Raise event?	Set to **y** to raise an event if conditions are met.
Log source	Specify the Application log.
Type: Error	Set to **y** to monitor for error events.
Event source filter	Specify the MSSQLSERVER event source.
Severity	Set to 28 to indicate a warning level event.
Action	In the **Action** field on the **Action** tab, select **Action_MapiMail**. With this setting, AppManager will notify you by email if any SQL Server events are detected.

To collect data and graph a trend chart from your System event log:

Properties and Parameters	How You Might Set Them
Schedule interval	On the **Schedule** tab, set the interval to once every hour.
Raise event?	Set to **y** to raise an event if conditions are met.
Collect data?	Set to **y** to collect data. AppManager will return the number of matching entries as the primary data point to be graphed. The first batch of filtered results can be viewed in the detail data message when you double-click on a data point. Additional matching entries may be included in the graph. The peaks and valleys in the graph indicate a large number of events (something unusual) or low event activity (quiet and all “OK”).
Log source	Specify the System log.
All other filters	not set
Action	Null

Sys_FailedLogon

Use this Knowledge Script to monitor the number of failed logon attempts to the server since the last interval. The result is always 0 for the first interval so that the script can establish a baseline for subsequent checks.

This script catches invalid `NET USE` attempts. It is generally believed that `NET USE` is a common way for hackers to break into a system using a password generator; repeated failed attempts to `NET USE` to a computer would indicate a possible attack. This script does not catch invalid Windows or IIS logons.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every one hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of `NET USE` attempts exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about `NET USE` attempts for graphs and reports. The default is n.
Threshold - Maximum failed logon attempts	Specify a threshold for the number of failed logon attempts. If the number of failed logon attempts exceeds the threshold, an event is raised. **Tip** If you find you are generating too many "insignificant" events from users entering passwords incorrectly, you may want to determine a "typical" log on failure pattern such as, five per 24 hours, and set this parameter accordingly.
Maximum number of entries per event report	Specify the maximum number of Application log events that can be returned in each event report. For example, if this value is set to 30 and 67 Application log events are found, then three event reports are raised: two reports containing 30 events and one report containing seven events. The default is 30. The Message column on the **Events** tab in the Operator Console displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 5.

Example of Using this Script

You can use this Knowledge Script to determine whether password-guessing programs are being used to crack the security on the server. This script can raise an event for each logon attempt that failed and collect data streams for the total number of logon failures.

Sys_FileChanged

Use this Knowledge Script to compare the size, timestamp, and attributes of a specified file from one interval to the next. This script raises an event if the file has been modified.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
File path	Enter the path of the file that you want to compare. The default path is `C:\temp\`
Raise event if file changes?	Set to **y** to raise an event if the file has changed. The default is y.
Check file size?	Set to **y** to compare the size of the file. The default is y.
Check file timestamp?	Set to **y** to compare the timestamp of the file. The default is y.
Check file attributes?	Set to **y** to compare the attributes of the file. The default is y.
Event severity when file size changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which file size changes. The default is 15.
Event severity when timestamp changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the timestamp changes. The default is 15.
Event severity when attributes change	Set the severity level, from 1 to 40, to indicate the importance of an event in which attributes change. The default is 15.

Sys_FilesCompare

Use this Knowledge Script to compare the size, timestamp, and attributes of two files. This script raises an event if differences are found.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
File path for first file	Enter the file path of the first file that you want to compare.
File path for second file	Enter the file path of the second file that you want to compare.
Raise event if sizes are different?	Set to **y** to raise an event if the sizes of the two files are different. The default is y.
Raise event if modification times are different?	Set to **y** to raise an event if the modification times of the two files are different. The default is y.
Raise event if attributes are different?	Set to **y** to raise an event if the attributes of the two files are different. The default is y.
Event severity when sizes are different	Set the severity level, from 1 to 40, to indicate the importance of an event in which the sizes of the two files are different. The default is 15.
Event severity when modification times are different	Set the severity level, from 1 to 40, to indicate the importance of an event in which the modification times of the two files are different. The default is 15.
Event severity when attributes are different	Set the severity level, from 1 to 40, to indicate the importance of an event in which the attributes of the two files are different. The default is 15.

Sys_GeneralCounter

Use this Knowledge Script to monitor any Performance Monitor counter. You can run this Knowledge Script on any machine or server, and can monitor any counter available in the Performance Monitor. You can set both high (Over) and low (Under) thresholds for the counter you are monitoring. You can set up the script to raise an event if the value of the counter you select is greater than the "Over threshold" value, or is less than the "Under threshold" value. You can also specify a consecutive number of times that the over or under threshold value must be exceeded before an event is raised.

This script raises an event only if the counter value is greater than the specified "Over threshold" value or is less than the specified "Under threshold" value. If a counter does not exist on the managed client, the Knowledge Script job terminates with an error.

To see a list of the counters available, click the **Browse** button in the **Counter to monitor** parameter or start the Performance Monitor and click the **Plus** [+] tool.

Note
This script differs from Sys_IntervalCounterin that it takes a "snapshot" of a counter when you run the script. IntervalCounter monitors the change in a counter between one run of the script and the next.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Set to **y** to collect data. The default is n.
Raise event if counter value exceeds the threshold?	Set to **y** to raise an event if the counter value is greater than the maximum threshold. The default is y.
Threshold - Maximum counter value	Enter a greater-than threshold for the counter value. If the counter you are monitoring exceeds this value, an event is raised. The default is 600.
Raise event if counter value falls below the threshold?	Set to **y** to raise an event if the counter value is less than the minimum threshold. The default is y.
Threshold - Minimum counter value	Enter a less-than threshold for the counter value. If the counter you are monitoring falls below this value, an event is raised. The default is 20.

Parameter	How To Set It
Counter to monitor	Select or enter the object, counter, and instances to monitor. **Note** If typing the counter name, use the format `<object>\<counter>\<instance>`. You can type multiple instances, separated by commas. For example: `Process\% Privileged Time\mapisp32,mqsvc` If the counter does not have an instance name, then end the string with a backslash: `Process\% Privileged Time\`. If an instance is a parent of multiple instances, for example, if you have a Logical Disk 0 with partitions C: and D:, type the complete instance name exactly as displayed in the Performance Monitor. For example "0 ==> C:".
Consecutive times	Specify the number of consecutive times the over or under threshold should be exceeded before an event is raised. The default is one time.
Event severity when counter value exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the counter value exceeds the threshold. The default is 8.
Event severity when counter value falls below the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the counter value falls below the threshold. The default is 8.
Event severity when no counter/instance is found	Set the severity level, from 1 to 40, to indicate the importance of an event in which no counter or instance is found. The default is 15.

Examples of Using this Script

Use this Knowledge Script to yield performance information for the counters you are interested in monitoring. When this script collects and graphs data, the results are similar to the results displayed in the Performance Monitor. With AppManager, you can use the counter data to start corrective actions when thresholds are exceeded, generate more complex and sophisticated graphs, and provide historical information for reporting, trend analysis, and capacity planning.

Simple counter with no instance name To monitor the Cache Hit Ratio counter and create one data stream, you can set the **Counter to monitor** parameter as follows: `SQLServer\Cache Hit Ratio`

For this type of counter you can simply leave the instance parameters blank.

To select this counter:

1. Click the **Browse** button.
2. Select the target Computer.
3. From the Object list, select **SQLServer**.
4. From the Counter list, select **Cache Hit Ratio**.
5. Click **OK**.

Counter with multiple identical instance names Assume you want to monitor the percentage of processor time used by several cmd processes running on a given computer. If you enter `cmd` as the instance name, only the first `cmd` process found is monitored.

To monitor additional `cmd` processes or select a specific `cmd` process rather than the "first found", you need to specify the instance index. The simplest way to select multiple instances is through the **Counter to monitor** parameter browser.

If you do not use the browser and there are multiple instances with the same name, you need to identify which instance to monitor using an instance index, with 0 indicating the first instance, 1 the second, and so on. If you do not enter an index, the first instance found is monitored. If you are typing the counter to monitor, use the format `<object>\<counter>\<instance> (<instance_index>)`. For example: `Process\% Privileged Time\cmd (0),cmd (1),cmd (3)`.

Counter with parent-child instances In some cases an instance is a parent of multiple child instances. For example, if you have a Logical Disk 0 with partitions C: and D:, the logical disk 0 is the parent of the logical disk C: and the logical disk D:. In addition, there may be multiple child instances with identical names. For example, two processes called MSDEV may each have threads 0, 1, 2, and 3:

```
Instance     ProcessID      ThreadID      Instance Index
MSDEV ==> 0    361            495               0
MSDEV ==> 0    291            426               1
MSDEV ==> 1    361            275               0
MSDEV ==> 1    291            181               1
MSDEV ==> 2    361            471               0
MSDEV ==> 2    291            256               1
MSDEV ==> 3    361            376               0
MSDEV ==> 3    291            500               1
```

The simplest way to select these child instances is through the Counter Browser. If you do not use the Counter Browser and there are child instances, you need to identify which instance to monitor using the format `<object>\<counter>\<parent_instance> ==> <child_instance>`. For example: `LogicalDisk\% Free Space\0 ==> C:`

If there are multiple child instances with the same name, you need to identify which child instances to monitor using an instance index, with 0 indicating the first instance, 1 the second, and so on. If you do not enter an index, the first instance found is monitored.

If you are entering the *Counter to monitor*, use the format: `<object>\<counter>\<parent> ==> <child> (<index>)`. For example: `Thread\% Processor Time\MSDEV ==> 0 (0),MSDEV ==> 0 (1)`.

Using the example above, this counter would retrieve `% Processor Time` for threads 495 (MSDEV process 361) and 426 (MSDEV process 291) and create two data streams.

```
ID   Job   KS Name          Legend
7    12    General_Counter  Thread-% Processor Time-MSDEV ==> 0(0)
6    12    General_Counter  Thread-% Processor Time-MSDEV ==> 0(1)
```

Format for entering counter names without browsing If you want to type counter names rather than use the Counter Browser, you need to enter the complete instance name exactly as it is displayed in the Performance Monitor, including any spaces or spelling conventions.

To manually set the **Counter to monitor** parameter without browsing, use one of the following formats:

Counter Type	General Format and Example
Single counter instance	`<object>\<counter>\<instance_name>` `Process\% Privileged Time\cmd`
Multiple instances	`<object>\<counter>\<instance> (<instance_index>)` `Process\% Privileged Time\cmd (1),cmd (4)`

Counter Type	General Format and Example
Child instances	<object>\<counter>\<parent_instance> ==> <child_instance> LogicalDisk\% Free Space\0 ==> C:
Multiple child instances	<object>\<counter>\<parent> ==> <child> (instance_index) Thread\% Processor Time\MSDEV ==> 0 (0),MSDEV ==> 0 (1)

Sys_IntervalCounter

Use this Knowledge Script to monitor the change in any Performance Monitor counter. You can run this Knowledge Script on any computer or server, and can monitor any counter available in the Performance Monitor. You can set high (Over) thresholds for the counter you are monitoring, as well as set up the script to raise an event if the value of the counter you select is greater than the *Counter delta value threshold* value. You can also specify a consecutive number of times that the *Counter delta value threshold* value must be exceeded before an event is raised.

This script automatically raises an event if it does not find the counter you want to monitor.

To see a list of the available counters, click the **Browse** button in the **Counter to monitor** parameter or start the Performance Monitor and click the **Plus** [+] tool.

Note
This script differs from Sys_GeneralCounterin that it monitors the change in a counter between one run of the script and the next. GeneralCounter takes a "snapshot" of a counter when you run the script.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Set to **y** to collect data about changes in counter values for reports and graphs. The default is n.
Raise event if threshold is exceeded?	Set to **y** to raise an event if the counter value change is greater than the threshold. The default is y.
Threshold - Maximum counter value change	Set the threshold for the maximum change that can occur between two counter values. The default is 600.
Counter to monitor	Select or enter the object, counter, and instance(s) to monitor. **Note** If typing the counter name, use the format `<object>\<counter>\<instance>`. You can enter multiple instances, separated by commas. For example: `Process\% Privileged Time\mapisp32,mqsvc`. If the counter does not have an instance name, then end the string with a backslash: `Process\% Privileged Time\`. If an instance is a parent of multiple instances, for example, if you have a Logical Disk 0 with partitions C: and D:, enter the complete instance name exactly as displayed in the Performance Monitor. For example "0 ==> C:".
Consecutive times	Specify the number of consecutive times the over or under threshold should be exceeded before an event is raised. The default is one time.

Parameter	How To Set It
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 8.
Event severity when no counter/instance is found	Set the severity level, from 1 to 40, to indicate the importance of an event in which no counter/instance is found. The default is 15.

Sys_LogicalDiskSpace

Use this Knowledge Script to monitor logical disk space usage. This script checks the percentage of disk space used and the amount of free space in megabytes. This script raises an event if usage exceeds the threshold or if free space falls below the threshold. In addition, this script generates data streams for disk space usage and available free space.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is breached?	Set to **y** to raise an event if a threshold is breached. The default is y.
Collect data?	Set to **y** to collect data about logical disk space usage for graphs and reports. The default is y.
Threshold - Maximum disk space usage	Specify the maximum percentage of disk space that can be in use before an event is raised. The default is 80%.
Threshold - Minimum free space available	Specify the minimum amount of disk space that should be available. If the amount of free space falls below the threshold, an event is raised. The default is 10 MB.
Event severity when threshold is breached	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is breached. The default is 8.

Sys_MemUtil

Use this Knowledge Script to monitor physical memory, virtual memory, and the paging files. This script raises an event if any usage level exceeds the threshold you set. In addition, this script generates data streams for physical memory, virtual memory, and page file size.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if physical memory usage exceeds the threshold?	Set to **y** to raise an event when physical memory usage exceeds the threshold you set. the default is y.
Raise event if virtual memory usage exceeds the threshold?	Set to **y** to raise an event when virtual memory usage exceeds the threshold you set. The default is y.
Raise event if paging file usage exceeds the threshold?	Set to **y** to raise an event when paging file usage exceeds the threshold you set. The default is y.
Collect data for physical memory?	Set to **y** to collect data about physical memory usage for graphs and reports. The default is n.
Collect data for virtual memory?	Set to **y** to collect data about virtual memory usage for graphs and reports. The default is n.
Collect data for paging file?	Set to **y** to collect data about paging file size for graphs and reports. The default is n.
Threshold - Maximum physical memory usage	Specify the maximum percentage of physical memory that can be in use before an event is raised. The default is 90%.
Threshold - Maximum virtual memory usage	Specify the maximum percentage of virtual memory that can be in use before an event is raised. The default is 90%.
Threshold - Maximum paging file usage	Specify the maximum percentage of the paging file that can be in use before an event is raised. The default is 70%.
Event severity when physical memory usage exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which physical memory usage exceeds the threshold. The default is 5.
Event severity when virtual memory usage exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which virtual memory usage exceeds the threshold. The default is 5.
Event severity when paging file usage exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which paging file usage exceeds the threshold. The default is 5.

Sys_PagingHigh

Use this Knowledge Script to monitor reads/writes per second to the pagefile. This script raises an event if the number of reads/writes per second exceeds the threshold you set. In addition, this script generates data streams for pagefile activity.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if pagefile activity exceeds the threshold?	Set to **y** to raise an event if pagefile activity exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about pagefile activity for graphs and reports. The default is n.
Threshold - Maximum pagefile activity per second	Specify the maximum number of reads/writes that can occur per second before an event is raised. The default is 200 per second.
Event severity when pagefile activity exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which pagefile activity exceeds the threshold. The default is 5.

Sys_ProcessDown

Use this Knowledge Script to determine whether specified processes are running. This script raises an event if a specified process is not running. In addition, this script generates data streams for process status: 100 for a running process; 0 for a non-running process.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if process is not running?	Set to **y** to raise an event if a specified process is not running. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. If set to **y**, the script returns data for each named process. A value of 100 is returned if the process is running; a value of 0 is returned if the process is not running. The default is n.
Processes to monitor	Type the names of one or more process that you want to monitor, separated by commas and no spaces. For example: `clock,tcpsvcs` **Note** Do not append .exe to the process names.
Event severity when process is not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which a specified process is not running. The default is 8.

Sys_Processes

Use this Knowledge Script to measure the number of current processes. This script raises an event if the number of processes exceeds the threshold that you set. In addition, this script generates a data stream for the number of processes.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the number of current processes exceeds the threshold. The default is y.
Collect data?	Set to y to collect data about processes for graphs and reports. The default is n.
Threshold - Maximum total processes	Specify the maximum number of processes that can be current before an event is raised. The default is 80.
Number of top processes to display	Specify the number of top processes you want to display in detail event or data message. Enter **0** if you want to display all processes. The default is 10.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of current processes exceeds the threshold. The default is 5.

Sys_ServiceChange

Use this Knowledge Script to detect any changes to the status and startup type of services. This script raises an event if the status (running, stopped, pending) or startup type (manual, automatic, disabled) of any service has changed. In addition, this script generates data streams for service status: 100 if the service is unchanged or 0 if the service is not running or has been changed.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if service changes?	Set to **y** to raise an event if the status or startup type of a service changes. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. If set to **y**, the script returns a value of 100 if the service is unchanged and a value of 0 if the service is not running or has been changed. The default is n.
Services to monitor	Type the names of services that you want to monitor, separated by commas and no spaces. You can type the internal service names or the service names displayed in the Control Panel. Type an asterisk (*) to check all services marked "Automatic." The default is `EventLog`.
Event severity when service start-type changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service start-type changes. The default is 10.
Event severity when service status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the service status changes. The default is 5.
Event severity when information retrieval fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which no service information can be retrieved. The default is 18.

Sys_ServiceDown

Use this Knowledge Script to check the status of user-specified services. This script raises an event if any detected service is not running, and can, if you want, restart the service. In addition, this script generates data streams for service status: 100 if the service is unchanged or 0 if the service is not running or has been changed.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise an event if service is down?	Set to **y** to raise an event if a specified service is down. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. If set to **y**, the script returns a value of 100 if the service is unchanged and a value of 0 if the service is not running or has been changed. The default is n.
Collect data only for down service?	Set to **y** to collect data only when a service is down. The default is n.
Services to monitor	Type the names of services you want to monitor, separated by commas and no spaces. You can type the internal service names or the service names displayed in the Control Panel. Type an asterisk (*) to check all services marked "Automatic." The default is `EventLog`.
Services to exclude	Type the names of services you want to exclude from monitoring, separated by commas and no spaces. You can type the internal service names or the service names displayed in the Control Panel.
Auto-start down service?	Set to **y** to automatically restart down services. The default is y.
Event severity when service is down/ auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a service is down and auto-start fails.
Event severity when service is down/ auto-start attempted	Set the severity level, from 1 to 40, to indicate the importance of an event in which a service is down and auto-start is attempted.
Event severity when service is down/ auto-start set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which a service is down and auto-start is set to “n.”
Event severity when service not found	Set the severity level, from 1 to 40, to indicate the importance of an event in which a specified service is not found.

Sys_ServiceHung

Use this Knowledge Script to detect whether any service is hung. A hung service is one in a Start-Pending, Stop-Pending, Continue-Pending or Pause-Pending state for a number of consecutive intervals. This script raises an event if any service is hung, and can, if you choose, stop or restart the service.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Services to monitor	Type the names of services you want to monitor, separated by commas and no spaces. You can type the internal service names or the service names displayed in the Control Panel. Type an asterisk (*) to check all services marked "Automatic." The default is `EventLog`.
Threshold - Maximum consecutive intervals	Specify the maximum number of consecutive times a service can be in a Start-Pending, Stop-Pending, Continue-Pending or Pause-Pending state before it is considered to be hung. The default is 2.
Raise event if threshold is exceeded?	Set to **y** to raise an event if a service is considered to be hung. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. If set to y, the script returns a value of 100 if the service is up and a value of 0 if the service is hung. The default is n.
Stop the hung service?	Set to **y** to automatically stop hung services. The default is y.
Auto-start stopped service?	Set to **y** to automatically restart stopped services. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which auto-start fails. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which auto-start succeeds. The default is 25.
Event severity when auto-start set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which auto-start is set to n. The default is 18.
Event severity when service status retrieval fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of a service could not be retrieved. The default is 10.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a hung service could not be stopped. The default is 10.

Sys_SystemUpTime

Use this Knowledge Script to monitor number of hours that a computer has been operational since it was last rebooted. This script raises an event if the computer was rebooted within the monitoring interval. In addition, this script generates data streams for system uptime.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if system is rebooted?	Set to **y** to raise an event if the system has been rebooted. The default is y.
Collect data?	Set to **y** to collect data for about system uptime for graphs and reports. The default is n.
Event severity when system is rebooted	Set the severity level, from 1 to 40, to indicate the importance of an event in which the system has been rebooted. The default is 8.

Sys_TopCpuProcs

Use this Knowledge Script to monitor the CPU resources used by all processes and to identify which processes use the most CPU resources. This script raises an event if CPU usage exceeds the threshold. In addition, this script generates data streams for CPU usage.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if CPU usage exceeds the threshold?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about CPU usage for graphs and reports. The default is n.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU resources that can be in use for all processes before an event is raised. The default is 90%.
Number of top processes to display	Specify the number of top processes you want displayed in the detail message (event or data). Enter 0 if you want all processes displayed. The default is 5. **Note** NetIQ Corporation recommends that you limit the number of processes included in the detail message to the top five to 10 processes, rather than reporting on all processes. In most cases, including all processes increases the size of the detail message without providing you with information that is more useful. Typically, the top few processes are the most significant and the most likely ones you are looking to track down for troubleshooting purposes.
Event severity when CPU usage exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 5.

Sys_TopMemoryProcs

Use this Knowledge Script to monitor the total memory in KB used by all processes, and to identify which processes use the most memory. This script raises an event if memory usage exceeds the threshold. In addition, this script generates data streams for memory usage.

Resource Object

NortelBCM_NT_MachineFolder

Default Schedule

The default schedule is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Raise event if memory usage exceeds the threshold?	Set to **y** to raise an event if memory usage exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data about memory usage for graphs and reports. The default is n.
Threshold - Maximum memory usage	Specify the maximum amount memory that should be in use for all processes before an event is raised. The default is 102400 KB.
Number of top processes to display	Specify the number of top processes you want displayed in the detail message (event or data). Enter 0 if you want all processes displayed. The default is 5. **Note** NetIQ Corporation recommends that you limit the number of processes included in the detail message to the top five to 10 processes, rather than reporting on all processes. In most cases, including all processes increases the size of the detail message without providing you with information that is more useful. Typically, the top few processes are the most significant and the most likely ones you are looking to track down for troubleshooting purposes.
Event severity when memory usage exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. The default is 5.

Chapter 49
NortelBCMx Knowledge Scripts

AppManager for Nortel BCMx provides the following Knowledge Scripts for monitoring Nortel BCM software version 4.0 or later on hardware models 200, 400 and 1000, and Nortel BCM firmware version 1.00.2.04j or greater on hardware model 50, including versions 50a and 50e. From within the Operator Console, select a Knowledge Script on the NortelBCMx tab in the Knowledge Script pane and press **F1** for complete details.

Knowledge Script	What It Does
Alarms	Monitors the Nortel BCMx proxy computer for Nortel BCM alarms.
CallByCallLimits	Monitors the number of incoming and outgoing calls denied because call-by-call limits were exceeded.
ChassisUsage	Monitors the physical chassis of a BCM device.
HealthCheck	Monitors the operational status of BCM services.
HuntGroupUsage	Monitors call statistics for one or more hunt groups.
InterfaceHealth	Monitors the operational status of the interfaces on a network device.
LinkUtilization	Monitors LAN links for utilization and packet errors.
LogicalDiskSpace	Monitors logical disk space usage and availability.
PSTNFallback	Monitors PSTN fallback attempts and failures.
QoSLog	Monitors the MOS estimates for several codecs: G.711a, G.711u, G.723 5.3. kbps, G.723 6.3 kbps, G.729, and G.729A.
SystemUpTime	Monitors the number of seconds that the system has been operational since its last reboot.
SystemUsage	Monitors BCM CPU and memory usage.
UPSHealth	Monitors any attached uninterruptible power supply.
Recommended Knowledge Script Group	Performs essential monitoring of your Nortel BCM environment.
Discovery_NortelBCMx	Discovers the various components of a Nortel BCM installation for software version 4.0 and hardware models 50, 50a, 50e, 200, 400, and 1000.

Alarms

Use this Knowledge Script to monitor the Nortel BCMx proxy computer for Nortel BCM alarms. Nortel BCM devices send alarms to the proxy computer using SNMP traps.

When setting parameters for this script, you are asked to provide a list of alarm identifiers (system messages) that you want to include or exclude from monitoring. Their format consists of a multi-digit alarm number, such as 18 or 10029.

Prerequisites

- Install the Windows SNMP service before running this script. If you installed the service before you installed the Nortel BCMx module that contains this script, you do not need to do anything else. If you installed the service after you installed the Nortel BCMx module, stop and restart the AppManager agent on the proxy agent computer before using this script.
- Configure Nortel BCM devices to send SNMP traps to the proxy agent. For more information, see "Identifying the SNMP Trap Receiver" on page 2904.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx

Default Schedule

By default, this script runs on an asynchronous schedule.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How to Set It
Notes for the alarm categories: • If you choose to "Include only" selected alarm identifiers in a category, AppManager will raise events *only* for those identifiers. *AppManager will not raise events for the other identifiers included in the category.* • If you choose to "Exclude" selected alarm identifiers from a category, AppManager will raise events for all alarm identifiers included in the category *except* those that you specifically excluded. • If you accept the default parameter settings, which are "Exclude" and blank (in the *Alarm identifiers* parameter), AppManager will raise events for all identifiers in the category, because you excluded nothing from the category.	
Monitor PVQM alarms?	Select **Yes** to monitor the Nortel BCMx proxy server for alarms in the "PVQM" category. The default is Yes.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers that you specify in the following parameter. By default, AppManager monitors all alarms with PVQM severity in the SNMP trap.

Parameter	How to Set It
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the “PVQM” category. By default, the list contains the 50501, 50504, 50507, and 50510 identifiers.
Monitor critical alarms?	Select **Yes** to monitor the Nortel BCMx proxy server for alarms in the “critical” category. The default is Yes.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. By default, AppManager monitors all alarms with critical severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the “critical” category. The default is an empty list.
Monitor major alarms?	Select **Yes** to monitor the Nortel BCMx proxy server for alarms in the “major” category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. By default, AppManager monitors all alarms with major severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the “major” category. The default is an empty list.
Monitor minor alarms?	Select **Yes** to monitor the Nortel BCMx proxy server for alarms in the “minor” category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. By default, AppManager monitors all alarms with minor severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the “minor” category. The default is an empty list.
Monitor warning alarms?	Select **Yes** to monitor the Nortel BCMx proxy server for alarms in the “warning” category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. By default, AppManager monitors all alarms with warning severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the “warning” category. The default is an empty list.
Monitor info alarms?	Select **Yes** to monitor the Nortel BCMx proxy server for alarms in the “informational” category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. By default, AppManager monitors all alarms with informational severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the “informational” category. The default is an empty list.
Event Severities	
Severity - Critical alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a critical alarm is detected. The default is 10.
Severity - Major alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a major alarm is detected. The default is 15.
Severity - Minor alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a minor alarm is detected. The default is 20.

Parameter	How to Set It
Severity - Warning alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a warning alarm is detected. The default is 25.
Severity - Info alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which an informational alarm is detected. The default is 30.

Identifying the SNMP Trap Receiver

Manually configure Nortel BCM to send SNMP traps to AppManager. Use Element Manager to identify the AppManager proxy computer as an SNMP trap receiver.

To identify the proxy computer as a trap receiver:

1. Log in to Element Manager.
2. On the Administration tab, expand the **General** folder and select **SNMP Trap Destinations**.
3. In the right pane, click **Add**, and then complete the fields as described in the table below:

Field	Instructions
Name	Provide the host name of the proxy agent computer to which you want to send SNMP traps (the computer on which the BCMx module is installed).
Host address	Provide the IP address of the proxy agent computer.
Port	Accept the default: port 162.
SNMP version	Accept the default: v1/v2C.
Community string	Provide the SNMP community string of the proxy agent computer.
User name	Leave this field blank.

4. Click **OK**.

CallByCallLimits

Use this Knowledge Script to monitor incoming and outgoing calls that were denied because call-by-call limits were exceeded. PRI pools that support call-by-call services have maximum and minimum call limits for each service. You can assess the capacity of the PRI call services on your system by monitoring the number of calls that were denied because they exceeded or fell below the limits.

This script raises an event when any monitored value exceeds a threshold that you set.

Call-by-call limits are programmed in Element Manager and are defined as follows:

Limit	Definition
Incoming maximum	The maximum number of calls that can enter the PRI pools for a particular service. Any calls that exceed the maximum will be denied.
Incoming minimum	The minimum number of calls that can enter the PRI pools for a particular service. If the number of calls falls below the minimum, the calls will be denied and the PRI pools will be allocated to a different service.
Outgoing maximum	The maximum number of calls that can exit the PRI pools for a particular service. Any calls that exceed the maximum will be denied.
Outgoing minimum	The minimum number of calls that can exit the PRI pools for a particular service. If the number of calls falls below the minimum, the calls will be denied and the PRI pools will be allocated to a different service.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx_PRIPool

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the CallByCallLimits job fails. The default is 5.
Monitor incoming calls denied after maximum limit exceeded	
Event Notification	

Parameter	How To Set It
Raise event if denied incoming calls exceed threshold?	Select **Yes** to raise an event if the number of denied incoming calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum denied incoming calls	Specify the highest number of incoming calls that can be denied before an event is raised. The default is 0 calls.
Event severity when denied incoming calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of denied incoming calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for incoming calls denied after maximum limit exceeded?	Select **Yes** to collect data about incoming calls that were denied after the maximum limit was exceeded. The default is unselected.
Monitor incoming calls denied after minimum limit not reached	
Event Notification	
Raise event if denied incoming calls exceed threshold?	Select **Yes** to raise an event if the number of denied incoming calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum denied incoming calls	Specify the maximum number of incoming calls that can be denied before an event is raised. The default is 0 calls.
Event severity when denied incoming calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of denied incoming calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for incoming calls denied after minimum limit not reached	Select **Yes** to collect data about incoming calls that were denied after the minimum limit was not reached. The default is unselected.
Monitor outgoing calls denied after maximum limit exceeded	
Event Notification	
Raise event if denied outgoing calls exceed threshold?	Select **Yes** to raise an event if the number of denied outgoing calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum denied outgoing calls	Specify the highest number of outgoing calls that can be denied before an event is raised. The default is 0 calls.
Event severity when denied outgoing calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of denied outgoing calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for outgoing calls denied after maximum limit exceeded?	Select **Yes** to collect data about outgoing calls that were denied after the maximum limit was exceeded. The default is unselected.
Monitor outgoing calls denied after minimum limit not reached	
Event Notification	
Raise event if denied outgoing calls exceed threshold?	Select **Yes** to raise an event if the number of denied outgoing calls exceeds the threshold that you set. The default is Yes.

Parameter	How To Set It
Threshold - Maximum denied outgoing calls	Specify the highest number of outgoing calls that can be denied before an event is raised. The default is 0 calls.
Event severity when denied outgoing calls exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of denied outgoing calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for outgoing calls denied after minimum limit not reached?	Select **Yes** to collect data about outgoing calls that were denied after the minimum limit was not reached. The default is unselected.

ChassisUsage

Use this Knowledge Script to monitor the physical chassis of a BCM device, including temperature sensors, voltage sensors, and fan speeds. This script raises events for status changes in BCM 200/400 components (running BCM software version 4.0) and for monitored values that exceed or fall below the threshold that you set. In addition, this script generates data streams for the following metrics:

- Remote temperature for BCM 50
- Local temperature
- CPU temperature for BCM 200/400
- Fan 1 and fan 2 speeds for BCM 50
- Power supply voltage levels:
  - v5
  - v+12
  - v-12 for BCM 200/400
  - vcc for BCM 50
  - vccp for BCM 50
  - v3.3 (Standby, One, and Two) for BCM 200/400

Notes

- BCM model 1000 does not support the monitoring of voltage, fan speed, or temperature. This script raises an event if you attempt to monitor any of these chassis components on BCM 1000.
- In this script, the monitoring of fan speeds, temperatures, and voltages is disabled by default. BCM itself will raise an alarm if any of these values is abnormal, and then send the alarm as an SNMP trap to the Alarms script. If you enable the monitoring of fan speeds, temperatures, or voltages, be aware that you may receive duplicate or conflicting alarm and events. For instance, AppManager may raise an event indicating a high temperature based on a threshold that you set, but the BCM does not raise an alarm because the temperature has not yet reached the abnormal level as determined by Nortel.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the ChassisUsage job fails. The default is 5.
The ChassisUsage script monitors status changes only for BCM 200/400 models running BCM software version 4.0. The event message indicates the type of change, such as "The status for local temperature has changed to Above Tolerance" or "The status of fan 1 has changed to Stopped."	
Raise event if local temperature status changes?	Select **Yes** to raise an event if the status of the local temperature changes. The default is unselected.
Event severity when local temperature status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the local temperature has changed. The default is 30.
Raise event if CPU temperature status changes?	Select **Yes** to raise an event if the status of the CPU temperature changes. The default is unselected.
Event severity when CPU temperature status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the CPU temperature has changed. The default is 30.
Raise event if fan 1 status changes?	Select **Yes** to raise an event if the status of fan 1 changes. The default is unselected.
Event severity when fan 1 status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of fan 1 has changed. The default is 30.
Raise event if CPU fan status changes?	Select **Yes** to raise an event if the status of the CPU fan changes. The default is unselected.
Event severity when CPU fan status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the CPU fan has changed. The default is 30.
Raise event if v5 voltage status changes?	Select **Yes** to raise an event if the status of the v5 power supply voltage changes. The default is unselected.
Event severity when v5 voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the v5 power supply voltage has changed. The default is 30.
Raise event if v+12 voltage status changes?	Select **Yes** to raise an event if the status of the v+12 power supply voltage changes. The default is unselected.
Event severity when v+12 voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the v+12 power supply voltage has changed. The default is 30.
Raise event if v-12 voltage status changes?	Select **Yes** to raise an event if the status of the v-12 power supply voltage changes. The default is unselected.
Event severity when v-12 voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the v-12 power supply voltage has changed. The default is 30.
Raise event if v3.3 Standby voltage status changes?	Select **Yes** to raise an event if the status of the v3.3 Standby power supply voltage changes. The default is unselected.
Event severity when v3.3 Standby voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the v3.3 Standby power supply voltage has changed. The default is 30.

Description	How To Set It
Raise event if v3.3 One voltage status changes?	Select **Yes** to raise an event if the status of the v3.3 One power supply voltage changes. The default is unselected.
Event severity when v3.3 One voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the v3.3 One power supply voltage has changed. The default is 30.
Raise event if v3.3 Two voltage status changes?	Select **Yes** to raise an event if the status of the v3.3 Two power supply voltage changes. The default is unselected.
Event severity when v3.3 Two voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the status of the v3.3 Two power supply voltage has changed. The default is 30.
Monitor local temperature	
Event Notification	
Raise event if local temperature exceeds threshold?	Select **Yes** to raise an event if the local temperature exceeds the threshold that you set. The default is unselected.
Threshold - Maximum local temperature	Specify the highest local temperature that can occur before an event is raised. The default is 55º Celsius.
Event severity when local temperature exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the local temperature exceeds the threshold. The default is 10.
Data Collection	
Collect data for local temperature?	Select **Yes** to collect data about local temperature for reports and graphs. The default is unselected.
Monitor remote temperature (BCM 50 only)	
Event Notification	
Raise event if remote temperature exceeds threshold?	Select **Yes** to raise an event if the remote temperature on a BCM 50 exceeds the threshold that you set. The default is unselected.
Threshold - Maximum remote temperature	Specify the highest remote temperature that can occur on a BCM 50 before an event is raised. The default is 55º Celsius.
Event severity when remote temperature exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the remote temperature on a BCM 50 exceeds the threshold. The default is 10.
Data Collection	
Collect data for remote temperature?	Select **Yes** to collect data about remote temperature for reports and graphs. The default is unselected.
Monitor CPU temperature (BCM 200/400 only)	
Event Notification	
Raise event if CPU temperature exceeds threshold?	Select **Yes** to raise an event if the CPU temperature on a BCM 200 or 400 exceeds the threshold that you set. The default is unselected.
Threshold - Maximum CPU temperature	Specify the highest CPU temperature that can occur on a BCM 200 or 400 before an event is raised. The default is 55º Celsius.
Event severity when CPU temperature exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CPU temperature on a BCM 200 or 400 exceeds the threshold. The default is 10.
Data Collection	

Description	How To Set It
Collect data for CPU temperature?	Select **Yes** to collect data about CPU temperature for reports and graphs. The default is unselected.
Monitor fan 1 speed (BCM 50 only)	
Event Notification	
Raise event if fan 1 speed exceeds threshold?	Select **Yes** to raise an event if the speed of fan 1 on a BCM 50 exceeds the threshold that you set. The default is unselected.
Threshold - Maximum fan 1 speed	Specify the highest fan speed that can occur before an event is raised. The default is 10000 RPMs.
Event severity when fan 1 speed exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the fan speed exceeds the threshold. The default is 10.
Data Collection	
Collect data for fan 1 speed?	Select **Yes** to collect data about fan speed for reports and graphs. The default is unselected.
Monitor fan 2 speed (BCM 50 only)	
Event Notification	
Raise event if fan 2 speed exceeds threshold?	Select **Yes** to raise an event if the speed of fan 2 on a BCM 50 exceeds the threshold that you set. The default is unselected.
Threshold - Maximum fan 2 speed	Specify the highest fan speed that can occur before an event is raised. The default is 10000 RPMs.
Event severity when fan 2 speed exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the fan speed exceeds the threshold. The default is 10.
Data Collection	
Collect data for fan 2 speed?	Select **Yes** to collect data about fan speed for reports and graphs. The default is unselected.
Monitor v5 voltage level	
Event Notification	
Raise event if v5 voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the v5 power supply voltage level exceeds or falls below the thresholds that you set. The default is unselected. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is unselected.
Threshold - Maximum v5 voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 5.25 volts.
Event severity when v5 voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum v5 voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 4.75 volts.
Event severity when v5 voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for v5 voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.

Description	How To Set It
Monitor v+12 voltage level	
Event Notification	
Raise event if v+12 voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the v+12 power supply voltage level exceeds or falls below the thresholds that you set. The default is unselected. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is unselected.
Threshold - Maximum v+12 voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 12.6 volts.
Event severity when v+12 voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum v+12 voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 11.4 volts.
Event severity when v+12 voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for v+12 voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.
Monitor v-12 voltage level (BCM 200/400 only)	
Event Notification	
Raise event if v-12 voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the v-12 power supply voltage level exceeds or falls below the thresholds that you set. The default is unselected. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is unselected.
Threshold - Maximum v-12 voltage level	Specify the highest voltage level that can occur before an event is raised. The default is -12.6 volts.
Event severity when v-12 voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum v-12 voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is -11.4 volts.
Event severity when v-12 voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for v-12 voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.
Monitor vcc voltage level (BCM 50 only)	
Event Notification	

Description	How To Set It
Raise event if vcc voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the vcc power supply voltage level exceeds or falls below the thresholds that you set. The default is unselected. vcc refers to voltage from a power supply connected to the collector terminal of a bipolar transistor. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is unselected.
Threshold - Maximum vcc voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 3.4 volts.
Event severity when vcc voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum vcc voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 3.2 volts.
Event severity when vcc voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for vcc voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.
Monitor vccp voltage level (BCM 50 only)	
Event Notification	
Raise event if vccp voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the vccp power supply voltage level exceeds or falls below the thresholds that you set. The default is unselected. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is unselected.
Threshold - Maximum vccp voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 1.442 volts.
Event severity when vccp voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum vccp voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 1.358 volts.
Event severity when vccp voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for vccp voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.
Monitor v3.3 Standby voltage level (BCM 200/400 only)	
Event Notification	
Raise event if v3.3 Standby voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the v3.3 Standby power supply voltage level exceeds or falls below the thresholds that you set. The default is Yes. **Note** You cannot enable an upper or lower threshold unless you check this option.

Description	How To Set It
Upper threshold	Select **Enable** to use an upper threshold value. The default is unselected.
Threshold - Maximum v3.3 Standby voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 3.4 volts.
Event severity when v3.3 Standby voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum v3.3 Standby voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 3.2 volts.
Event severity when v3.3 Standby voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for v3.3 Standby voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.
Monitor v3.3 One voltage level (BCM 200/400 only)	
Event Notification	
Raise event if v3.3 One voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the v3.3 One power supply voltage level exceeds or falls below the thresholds that you set. The default is Yes. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is Unchecked.
Threshold - Maximum v3.3 One voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 3.4 volts.
Event severity when v3.3 One voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is unselected.
Threshold - Minimum v3.3 One voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 3.2 volts.
Event severity when v3.3 One voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for v3.3 One voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.
Monitor v3.3 Two voltage level (BCM 200/400 only)	
Event Notification	
Raise event if v3.3 Two voltage level exceeds or falls below threshold?	Select **Yes** to raise an event if the v3.3 Two power supply voltage level exceeds or falls below the thresholds that you set. The default is Yes. **Note** You cannot enable an upper or lower threshold unless you check this option.
Upper threshold	Select **Enable** to use an upper threshold value. The default is Unchecked.
Threshold - Maximum v3.3 Two voltage level	Specify the highest voltage level that can occur before an event is raised. The default is 3.4 volts.

Description	How To Set It
Event severity when v3.3 Two voltage level exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is Unchecked.
Threshold - Minimum v3.3 Two voltage level	Specify the lowest voltage level that can occur before an event is raised. The default is 3.2 volts.
Event severity when v3.3 Two voltage level falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the voltage level falls below the threshold. The default is 10.
Data Collection	
Collect data for v3.3 Two voltage level?	Select **Yes** to collect data about voltage level for reports and graphs. The default is unselected.

HealthCheck

Use this Knowledge Script to monitor the operational status of Nortel BCM services. A data point of 100 is recorded if the service is running; a data point of 0 is recorded if the service is not running. Possible non-running states include start pending, stopped, stop pending, continue pending, paused, and pause pending.

This script raises an event when a monitored value exceeds a threshold that you set.

It is important to monitor the up-and-down status of vital Nortel BCM services. If any service consumes excessive CPU resources, other services may be adversely affected. Run this script to notify you when a critical service goes down or when the overall percentage of important services drops below the specified threshold. The BCM Reset utility should restart any down service in a timely manner.

Monitored Services

The HealthCheck script monitors the operational status of several BCM services. In addition, the script can be configured to monitor the availability percentage of key services. The following table identifies the services that you can monitor with HealthCheck.

Service Name	Description	Key?
BackupRestoreProviderAgent	CIMOM Provider	
BCM_DataInterfacesProviderAgent	CIMOM Provider	
BCM_DCMProviderAgent	CIMOM Provider	
BCM_DNSProviderAgent	CIMOM Provider	
BCM_Doorphone	CIMOM Provider	
BCM_HostProviderAgent	CIMOM Provider	
BCM_IPMusicProviderAgent	CIMOM Provider	
BCM_ISDNProviderAgent	CIMOM Provider	
BCM_LicenseProviderAgent	CIMOM Provider	
BCM_LogProviderAgent	CIMOM Provider	
BCM_MIB2ProviderAgent	CIMOM Provider	
BCM_ModemDialUpProviderAgent	CIMOM Provider	
BCM_NetLinkMgrProviderAgent	CIMOM Provider	
BCM_NetworkInterfacesProviderAgent	CIMOM Provider	
BCM_PPPoEProviderAgent	CIMOM Provider	
BCM_PSM_ProviderAgent	CIMOM Provider	
BCM_RASProviderAgent	CIMOM Provider	
BCM_RoutingProviderAgent	CIMOM Provider	
BCM_SecurityProviderAgent	CIMOM Provider	
BCM_SNMPProviderAgent	CIMOM Provider	
BCM_SRGProviderAgent	CIMOM Provider	
BCM_TimeServiceProviderAgent	CIMOM Provider	
BCM_TimeZoneSettingProviderAgent	CIMOM Provider	
BCM_WANProviderAgent	CIMOM Provider	

Service Name	Description	Key?
BCM_WebCacheProviderAgent	CIMOM Provider	
BcmAmp	IP Music	
BCMCoreUploadProviderAgent	CIMOM Provider	
BCMInventoryProviderAgent	CIMOM Provider	
BCMPerfMonProviderAgent	CIMOM Provider	
BCMSystemProviderAgent	CIMOM Provider	
BCMUPSProviderAgent	CIMOM Provider	
BCMWebProviderAgent	CIMOM Provider	
btraceserver	Plug-in for Authentication and Routing Management for BT	
CallPilotProviderAgent	CIMOM Provider	
CCRSAppServer	Call Center Reporting Service	Yes
CDRProviderAgent	CIMOM Provider	
CDRService	Call Detail Recording service	
cfsserver	Component Feature service	Yes
core_file_monitor	Core File Monitor	
coreauthservice	CoreTel Authentication Service	
CoreTel	Main Telephony Process	Yes
CoreTelProviderAgent	CIMOM Provider	
crond	CRON Scheduler Daemon	
Cte	Computer Telephony Engine	
ctiserver	Computer Telephony Integration	Yes
DataDebugToolsProviderAgent	CIMOM Provider	
dhcpd	DHCP Server Daemon	Yes
DHCPProviderAgent	CIMOM Provider	
DiaLogger	System Logging Mechanism	
DSCProviderAgent	CIMOM Provider	
EchoServer	Echo Server	
feps	Functional Endpoint Proxy Server	Yes
gated	Router SNMP Subagent	
HGMetricsReporter	Hunt Group Metrics	
HotDesking	used with IP sets	
httpd	http Daemon	
ipppd.ippp0-15	Router/WAN Services	Yes
IPSecProviderAgent	CIMOM Provider	
IpTelProviderAgent	CIMOM Provider	
IVRProviderAgent	CIMOM Provider	
LanCteProviderAgent	CIMOM Provider	

Service Name	Description	Key?
LANProviderAgent	CIMOM Provider	
lms	Line Monitor Server	
LogManagement	Log File Management Service	
mgs	Media Gateway Server	Yes
mmdp	IVR Service	Yes
modemcc	Modem Call Control	Yes
monit	Monitoring Daemon	
mps	IP Telephony - Media Path	Yes
MscService	Media Services Card Service	Yes
Msm	Media Services Manager	Yes
MsmProviderAgent	CIMOM Provider	
NetworkStatisticsProviderAgent	CIMOM Provider	
NnuScheduler	System Scheduler	
owcimomd	Open WBEM CIMOM Server Daemon	Yes
Pdrd	Persistence Data Repository service	Yes
psm	Process Status Monitor service	Yes
qmond	QoS Monitor	
RAIDProviderAgent	CIMOM Provider	
securityservice	Authentication and Authorization	
snmpd	SNMP Server Daemon	
SoftwareUpdateProviderAgent	CIMOM Provider	
srg	Survivable Remote Gateway Service	Yes
srp	IVR Service	Yes
ssba	System Set Based Admin service	Yes
sshd	Secure Shell Daemon	
SyslogListener	Syslog Receiver	
tmwservice	Time service	
ToneSrvr	Tone Server	
utps	UniSTIM Terminal Proxy Server	Yes
voicemail	Voice Mail Process	Yes
Wan	WAN Service	Yes

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx

Default Schedule

The default interval for this script is 12 minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the HealthCheck job fails. The default is 5.
Raise event if services are not available?	Select **Yes** to raise an event if any monitored service is not available. The default is Yes.
Event severity when services are not available	Set the severity level, from 1 to 40, to indicate the importance of an event in which a monitored service is not available. The default is 10.
Monitor Key Service Availability	
Event Notification	
Raise event if key service availability falls below threshold?	Select **Yes** to raise an event if the percentage of key service availability falls below the threshold that you set. The default is Yes.
Threshold - Minimum key service availability	Specify the lowest percentage of key service availability that can occur before an event is raised. The default is 100%.
Event severity when key service availability falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of key service availability falls below the threshold. The default is 10.
Data Collection	
Collect data for key service availability?	Select **Yes** to collect data about key service availability for reports and graphs. The default is unselected.

HuntGroupUsage

Use this Knowledge Script to monitor call statistics for one or more hunt groups: busy percentage, abandoned percentage, average time in queue, and overflow percentage. This script raises an event if any monitored value exceeds the threshold that you set. In addition, this script generates data streams for percentage of abandoned calls, percentage of busy calls, overflow percentage, average time in queue, total calls, and total answers.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx_HuntGroup

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the HuntGroupUsage job fails. The default is 5.
Monitor Abandoned Percentage	
Event Notification	
Raise event if abandoned percentage exceeds threshold?	Select **Yes** to raise an event if the percentage of abandoned calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum abandoned percentage	Specify the highest percentage of abandoned calls that can occur before an event is raised. The default is 5%.
Event severity when abandoned percentage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of abandoned calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for abandoned percentage?	Select **Yes** to collect data about the percentage of abandoned calls for reports and graphs. The default is unselected.
Monitor Busy Percentage	
Event Notification	

Description	How To Set It
Raise event if busy percentage exceeds threshold?	Select **Yes** to raise an event if the percentage of busy calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum busy percentage	Specify the highest percentage of busy calls that can occur before an event is raised. The default is 5%.
Event severity when busy percentage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of busy calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for busy percentage?	Select **Yes** to collect data about the percentage of busy calls for reports and graphs. The default is unselected.
Monitor Overflow Percentage	
Event Notification	
Raise event if overflow percentage exceeds threshold?	Select **Yes** to raise an event if the percentage of overflow calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum overflow percentage	Specify the highest percentage of overflow calls that can occur before an event is raised. The default is 25%.
Event severity when overflow percentage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of overflow calls exceeds the threshold. The default is 10.
Data Collection	
Collect data for overflow percentage?	Select **Yes** to collect data about the percentage of overflow calls for reports and graphs. The default is unselected.
Monitor Average Time in Queue	
Event Notification	
Raise event if average time in queue exceeds threshold?	Select **Yes** to raise an event if the average time calls spend in queue exceeds the threshold that you set. The default is Yes.
Threshold - Maximum average time in queue	Specify the longest average time that calls can spend in queue before an event is raised. The default is 45 seconds.
Event severity when average time in queue exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average time calls spend in queue exceeds the threshold. The default is 10.
Data Collection	
Collect data for average time in queue?	Select **Yes** to collect data about average queue time for reports and graphs. The default is unselected.
Monitor Total Calls	
Data Collection	
Collect data for total calls?	Select **Yes** to collect data about the total number of calls for reports and graphs. The default is unselected.
Monitor Total Answers	
Data Collection	
Collect data for total answers?	Select **Yes** to collect data about the total number of answered calls for reports and graphs. The default is unselected.

InterfaceHealth

Use this Knowledge Script to monitor the operational status of interfaces for a BCM. This script raises an event when interface status changes. In addition, this script generates a data stream for interface availability.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx_LANLink

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the InterfaceHealth job fails. The default is 5.
Raise event if interface goes down?	Select **Yes** to raise an event if interface status changes to “down.” The default is Yes.
Event severity when interface is down	Set the severity level, from 1 to 40, to indicate the importance of an event in which interface status changes to “down.” The default is 5.
Raise event if interface comes up?	Select **Yes** to raise an event if an interface’s status changes to “up.” The default is Yes.
Event severity when interface is up	Set the severity level, from 1 to 40, to indicate the importance of an event in which interface status changes to “up.” The default is 30.
Monitor Interface Availability	
Data Collection	
Collect data for interface availability?	Select **Yes** to collect data about interface availability for reports and graphs. If enabled, data collection returns a value of 100 if the interface is available or a value of 0 if the interface is not available. The default is unselected.

LinkUtilization

Use this Knowledge Script to monitor LAN links on a BCM. This script monitors bandwidth utilization (including inbound and outbound utilization), bytes sent and received (bytes per second since the last polling period), and percentage of packet errors.

This script raises an event when a monitored value exceeds the threshold that you set. In addition, this script generates data streams for bandwidth utilization, packet errors, outbound bandwidth utilization, inbound bandwidth utilization, sent bytes, and received bytes.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

For both modes, this script can monitor packet errors, sent bytes, and received bytes. It cannot monitor bandwidth utilization for either mode.

Resource Object

Nortel_BCMx_LANLink

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the LinkUtilization job fails. The default is 5.
Monitor Bandwidth Utilization	
Event Notification	
Raise event if bandwidth utilization exceeds threshold?	Select **Yes** to raise an event if bandwidth (inbound and outbound) utilization exceeds the threshold that you set. The default is Yes.
Threshold - Maximum bandwidth utilization	Specify the highest percentage of bandwidth utilization that can occur before an event is raised. The default is 50%.
Event severity when bandwidth utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which bandwidth utilization exceeds the threshold. The default is 10.
Data Collection	
Collect data for bandwidth utilization?	Select **Yes** to collect data about inbound and outbound bandwidth utilization for reports and graphs. The default is unselected.
Monitor Packet Errors	

Description	How To Set It
Event Notification	
Raise event if packet errors exceed threshold?	Select **Yes** to raise an event if the percentage of packet errors exceeds the threshold that you set. The default is Yes. **Hint** When a packet is dropped during a VoIP transmission, a conversation can lose an entire syllable or word. Obviously, data loss can severely impair call quality. Set this parameter to **Yes** to receive immediate notification of packet loss that exceeds the threshold that you set.
Threshold - Maximum packet errors	Specify the highest percentage of packet errors that can occur before an event is raised. The default is 8%.
Event severity when packet errors exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of packet errors exceeds the threshold. The default is 10.
Data Collection	
Collect data for packet errors?	Select **Yes** to collect data about the percentage of packet errors for reports and graphs. The default is unselected.
Monitor Outbound Bandwidth Utilization	
Event Notification	
Raise event if outbound bandwidth utilization exceeds threshold?	Select **Yes** to raise an event if outbound bandwidth utilization exceeds the threshold that you set. The default is Yes.
Threshold - Maximum outbound bandwidth utilization	Specify the highest percentage of outbound bandwidth utilization that can occur before an event is raised. The default is 50%.
Event severity when outbound bandwidth utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which outbound bandwidth utilization exceeds the threshold. The default is 10.
Data Collection	
Collect data for outbound bandwidth utilization?	Select **Yes** to collect data about the percentage of outbound bandwidth utilization for reports and graphs. The default is unselected.
Monitor Inbound Bandwidth Utilization	
Event Notification	
Raise event if inbound bandwidth utilization exceeds threshold?	Select **Yes** to raise an event if inbound bandwidth utilization exceeds the threshold that you set. The default is Yes.
Threshold - Maximum inbound bandwidth utilization	Specify the highest percentage of inbound bandwidth utilization that can occur before an event is raised. The default is 50%.
Event severity when inbound bandwidth utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which inbound bandwidth utilization exceeds the threshold. The default is 10.
Data Collection	
Collect data for inbound bandwidth utilization?	Select **Yes** to collect data about the percentage of inbound bandwidth utilization for reports and graphs. The default is unselected.
Monitor Bytes Sent	
Data Collection	
Collect data for bytes sent?	Select **Yes** to collect data about the number of bytes sent per second for reports and graphs. The default is unselected.

Description	How To Set It
Monitor Bytes Received	
Data Collection	
Collect data for bytes received?	Select **Yes** to collect data about the number of bytes received per second for reports and graphs. The default is unselected.

LogicalDiskSpace

Use this Knowledge Script to monitor logical disk space usage and availability. This script raises an event when any monitored value exceeds a threshold that you set. In addition, this script generates data streams for used disk space and available disk space.

Resource Object

Nortel_BCMx_LogicalDisk

The LogicalDiskSpace Knowledge Script is a member of the NortelBCMx Recommended Knowledge Script Group (KSG), which allows you to run all recommended scripts at one time. However, there are limits on the number of Logical Disk objects on which the LogicalDiskSpace script can run. If you run the KSG on more objects than the LogicalDiskSpace script allows, you will receive an error message indicating that the number of target objects has exceeded its limit. If you receive this error message, remove the LogicalDiskSpace script from the KSG and run LogicalDiskSpace alone on fewer Logical Disk resources.

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the LogicalDiskSpace job fails. The default is 5.
Monitor Used Disk Space	
Event Notification	
Raise event if used disk space exceeds threshold?	Select **Yes** to raise an event if the amount of used disk space exceeds the threshold that you set. The default is Yes.
Threshold - Maximum used disk space	Specify the highest percentage of disk space that can be used before an event is raised. The default is 80%.
Event severity when used disk space exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which used disk space exceeds the threshold. The default is 10.
Data Collection	
Collect data for used disk space?	Select **Yes** to collect data about used disk space for reports and graphs. The default is unselected.
Monitor Available Disk Space	
Event Notification	
Raise event if available disk space falls below threshold?	Select **Yes** to raise an event if available disk space falls below the threshold that you set. The default is Yes.

Description	How To Set It
Threshold - Minimum available disk space	Specify the lowest amount of disk space that can be available before an event is raised. The default is 10 MB.
Event severity when available disk space falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which available disk space falls below the threshold. The default is 10.
Data Collection	
Collect data for available disk space	Select **Yes** to collect data about available disk space for reports and graphs. The default is unselected.

PSTNFallback

Use this Knowledge Script to monitor the number of PSTN (Public Switched Telephone Network) fallback attempts and failures that have occurred since the last polling period. Attempts are calls that were not able to route through the preferred trunk. Failures are calls that were not able to route through the fallback trunk.

This script raises an event when any monitored value exceeds a threshold that you set. In addition, this script generates data streams for PSTN fallback attempts and failures.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx_TelephonyFolder

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the PSTNFallback job fails. The default is 5.
Monitor PSTN Fallback Attempts	
Event Notification	
Raise event if PSTN fallback attempts exceed threshold?	Select **Yes** to raise an event if the number of fallback attempts exceeds the threshold that you set. The default is Yes.
Threshold - Maximum PSTN fallback attempts	Specify the highest number of fallback attempts that can occur before an event is raised. The default is 0 attempts.
Event severity when PSTN fallback attempts exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of fallback attempts exceeds the threshold. The default is 20.
Data Collection	
Collect data for PSTN fallback attempts	Select **Yes** to collect data about the number of fallback attempts for reports and graphs. The default is unselected.
Monitor PSTN Fallback Failures	
Event Notification	

Description	How To Set It
Raise event if PSTN fallback failures exceed threshold?	Select **Yes** to raise an event if the number of fallback failures exceeds the threshold that you set. The default is Yes.
Threshold - Maximum PSTN fallback failures	Specify the highest number of fallback failures that can occur before an event is raised. The default is 0 failures.
Event severity when PSTN fallback failures exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of fallback failures exceeds the threshold. The default is 10.
Data Collection	
Collect data for available PSTN fallback failures	Select **Yes** to collect data about the number of fallback failures for reports and graphs. The default is unselected.

QoSLog

Use this Knowledge Script to monitor the MOS estimates for several codecs: G.711a, G.711u, G.723 5.3 kbps, G.723 6.3 kbps, and G.729 and G.729A (in the outgoing call direction only). This script raises an event if any MOS estimate falls below the threshold you set. In addition, this script generates data streams for MOS estimates for each monitored codec.

If you use VoIP trunks, run this script to gather information from the BCM QoS Monitor log in order to verify that QoS between target BCMs is maintaining acceptable MOS. For more information, see "Understanding the Mean Opinion Score" on page 2933.

Prerequisite

Enable the QoS Monitor to log MOS scores. For more information, see "Enabling QoS Monitor" on page 2932.

Resource Object

Nortel_BCMx_TelephonyFolder

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QOSLog job fails. The default is 5.
Raise event if QoS monitor is not running from device?	Select **Yes** to raise an event if QoS Monitor is not running. The default is Yes. The QoS Monitor must be running in order to log the MOS scores this script monitors.
Event severity when QoS monitor is not running from device	Set the severity level, from 1 to 40, to indicate the importance of an event in which QoS Monitor is not running. The default is 5.
Monitor G.711a MOS	
Event Notification	
Raise event if G.711a MOS falls below threshold?	Select **Yes** to raise an event if the MOS for the G.711a codec falls below the threshold that you set. The default is Yes.
Threshold - Minimum G.711a MOS	Specify the lowest MOS that can occur before an event is raised. The default is 3.60.
Event severity when G.711a MOS falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS falls below the threshold. The default is 5.
Data Collection	

Description	How To Set It
Collect data for G.711a MOS?	Select **Yes** to collect data about G.711a MOS for reports and graphs. The default is unselected.
Monitor G.711u MOS	
Event Notification	
Raise event if G.711u MOS falls below threshold?	Select **Yes** to raise an event if the MOS for the G.711u codec falls below the threshold that you set. The default is Yes.
Threshold - Minimum G.711u MOS	Specify the lowest MOS that can occur before an event is raised. The default is 3.60.
Event severity when G.711u MOS falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS falls below the threshold. The default is 5.
Data Collection	
Collect data for G.711u MOS?	Select **Yes** to collect data about G.711u MOS for reports and graphs. The default is unselected.
Monitor G.723 5.3 kbps MOS	
Event Notification	
Raise event if G.723 5.3 kbps MOS falls below threshold?	Select **Yes** to raise an event if the MOS for the G.723 5.3 kbps codec falls below the threshold that you set. The default is Yes.
Threshold - Minimum G.723 5.3 kbps MOS	Specify the lowest MOS that can occur before an event is raised. The default is 3.60.
Event severity when G.723 5.3 kbps MOS falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS falls below the threshold. The default is 5.
Data Collection	
Collect data for G.723 5.3 kbps MOS?	Select **Yes** to collect data about G.723 5.3 kbps MOS for reports and graphs. The default is unselected.
Monitor G.723 6.3 kbps MOS	
Event Notification	
Raise event if G.723 6.3 kbps MOS falls below threshold?	Select **Yes** to raise an event if the MOS for the G.723 6.3 kbps codec falls below the threshold that you set. The default is Yes.
Threshold - Minimum G.723 6.3 kbps MOS	Specify the lowest MOS that can occur before an event is raised. The default is 3.60.
Event severity when G.723 6.3 kbps MOS falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS falls below the threshold. The default is 5.
Data Collection	
Collect data for G.723 6.3 kbps MOS?	Select **Yes** to collect data about G.723 6.3 kbps MOS for reports and graphs. The default is unselected.
Monitor G.729 MOS	
Event Notification	
Raise event if G.729 MOS falls below threshold?	Select **Yes** to raise an event if the MOS for the G.729 codec falls below the threshold that you set. The default is Yes.
Threshold - Minimum G.729 MOS	Specify the lowest MOS that can occur before an event is raised. The default is 3.60.

Description	How To Set It
Event severity when G.729 MOS falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS falls below the threshold. The default is 5.
Data Collection	
Collect data for G.729 MOS?	Select **Yes** to collect data about G.729 MOS for reports and graphs. The default is unselected.
Monitor G.729A MOS	
Event Notification	
Raise event if G.729A MOS falls below threshold?	Select **Yes** to raise an event if the MOS for the G.729A codec falls below the threshold that you set. The default is Yes.
Threshold - Minimum G.729A MOS	Specify the lowest MOS that can occur before an event is raised. The default is 3.60.
Event severity when G.729A MOS falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the MOS falls below the threshold. The default is 5.
Data Collection	
Collect data for G.729A MOS?	Select **Yes** to collect data about G.729A MOS for reports and graphs. The default is unselected.

Enabling QoS Monitor

If you use VoIP trunks, enable QoS Monitor in BCM before running the QoSLog Knowledge Script.

To enable QoS Monitor:

1. Log in to Element Manager.
2. On the Administration tab, expand **System Metrics** (for BCM 50 devices) or **System Status** (for BCM 4.0 devices), and then select **QoS Monitor**.
3. From the **Monitoring mode** list, select **Enabled in QoS-Monitor mode**.

For more information about VoIP trunks, see the "VoIP trunk gateways" chapter of the *Networking Configuration Guide* for your BCM device. For information about enabling the QoS Monitor, see the *Administration Guide* for your BCM device.

Understanding Codecs

In a VoIP transmission, the codec samples the sound and determines the data rate. A codec converts analog signals to digital (outbound) and digital signals to analog (inbound) for voice transmissions, and compresses (outbound) and decompresses (inbound) the digital information.

If you use VoIP trunks, use the QoSLog Knowledge Script to monitor the Mean Opinion Score (MOS) for six codec types. For more information, see "Understanding the Mean Opinion Score" on page 2933.

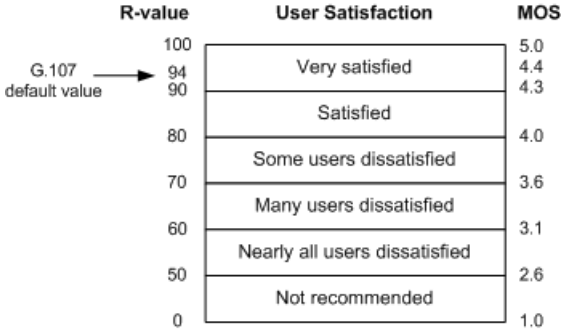
Codec	Description
G.711a	ITU standard for H.323-compliant codecs. Uses the A-law for companding, a popular standard in Europe.
G.711u	ITU standard for H.323-compliant codecs. Uses the U-law for companding, the most frequently used method in North America.

Codec	Description
G.723-5.3 kbps	Dual-rate speech codec for multimedia communications transmitting at 5.3 kbps. Uses the conjugate structure algebraic code excited linear predictive compression (ACELP) algorithm.
G.723-6.3 kbps	Dual-rate speech codec for multimedia communications transmitting at 6.3 kbps. Uses the multipulse maximum likelihood quantization (MPMLQ) compression algorithm.
G.729	High-performing codec that offers compression with high quality.
G.729A	Less-complex version of the G.729 codec. Developed for simultaneous voice and data applications for which the G.729 codec was too complex. Speech quality is virtually indistinguishable between G.729 and G.729A.

Understanding the Mean Opinion Score

The Mean Opinion Score (MOS) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. A modified version of the ITU (International Telecommunications Union) G.107 standard E-model equation is used to calculate the MOS. This algorithm is used to evaluate the quality of a transmission by factoring in the "mouth to ear" characteristics of a speech path.

The E-model is a complex calculation, the output of which is a single score called an R-value that is derived from delays and equipment impairment factors. An R-value can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor). As shown below, an estimated MOS can be calculated directly from an R-value:



SystemUpTime

Use this Knowledge Script to monitor the number of seconds that the BCM has been operational since its last reboot. This script raises an event if the system has rebooted. In addition, this script generates a data stream for system availability.

You want to be informed when your BCM has been rebooted. While a BCM is rebooting, calls are not going through. Knowing that the BCM has been rebooted can help prepare you for calls from disgruntled users whose calls were incomplete.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the SystemUpTime job fails. The default is 5.
Raise event if system has rebooted?	Select **Yes** to raise an event if the BCM has been rebooted. The default is Yes.
Event severity when system has rebooted	Set the severity level, from 1 to 40, to indicate the importance of an event in which the BCM has been rebooted. The default is 10.
Monitor System Up Time	
Data Collection	
Collect data for system up time?	Select **Yes** to collect data about system up time (number of seconds that the BCM has been powered on or since its last reboot) for reports and graphs. The default is unselected.

SystemUsage

Use this Knowledge Script to monitor the total CPU usage and memory usage for the BCM. This script raises an event when any monitored value exceeds a threshold that you set. In addition, this script generates data streams for CPU usage and memory usage.

Monitoring in SRG Mode

This script supports BCM 50 hardware running Nortel Survivable Remote Gateway (SRG) software, including instances when the SRG shifts to local mode for any reason.

Resource Object

Nortel_BCMx

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the SystemUsage job fails. The default is 5.
Monitor CPU Usage	
Event Notification	
Raise event if CPU usage exceeds threshold?	Select **Yes** to raise an event if CPU usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum CPU usage	Specify the highest CPU usage that can occur before an event is raised. The default is 80%.
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 10.
Data Collection	
Collect data for CPU usage?	Select **Yes** to collect data about CPU usage for reports and graphs. The default is unselected.
Monitor Memory Usage	
Event Notification	
Raise event if memory usage exceeds threshold?	Select **Yes** to raise an event if memory usage exceeds the threshold that you set. The default is Yes.
Threshold - Maximum memory usage	Specify the highest memory usage that can occur before an event is raised. The default is 80%.
Event severity when memory usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. The default is 10.

Description	How To Set It
Data Collection	
Collect data for memory usage?	Select **Yes** to collect data about memory usage for reports and graphs. The default is unselected.

UPSHealth

Use this Knowledge Script to monitor an attached uninterruptible power supply (UPS) for changes in operational status, load status, temperature status, and output and input voltage statuses, as well as temperature, load, and output and input voltage.

By warning you of changes to UPS status, this script can help you prevent outages that affect your users.

This script raises an event if a monitored status changes or if a monitored value exceeds a threshold that you set. In addition, this script generates data streams for UPS temperature, UPS load, UPS output voltage, and UPS input voltage.

Resource Object

Nortel_BCMx_UPS

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed.

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event raised when the UPSHealth job fails. The default is 5.
Raise event if UPS operational status changes?	Select **Yes** to raise an event if the UPS operational status changes. The default is unselected.
Event severity when UPS operational status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UPS operational status changes. The default is 30.
Raise event if UPS temperature status changes?	Select **Yes** to raise an event if the UPS temperature status changes. The default is unselected.
Event severity when UPS temperature status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UPS temperature status changes. The default is 30.
Raise event if UPS load status changes?	Select **Yes** to raise an event if the UPS load status changes. The default is unselected.
Event severity when UPS load status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UPS load status changes. The default is 30.
Raise event if UPS output voltage status changes?	Select **Yes** to raise an event if the UPS output voltage status changes. The default is unselected.
Event severity when UPS output voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UPS output voltage status changes. The default is 30.

Description	How To Set It
Raise event if UPS input voltage status changes?	Select **Yes** to raise an event if the UPS input voltage status changes. The default is unselected.
Event severity when UPS input voltage status changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which the UPS input voltage status changes. The default is 30.
Monitor Temperature	
Event Notification	
Raise event if temperature exceeds threshold?	Select **Yes** to raise an event if the UPS temperature exceeds the threshold that you set. The default is Yes.
Threshold - Maximum temperature	Specify the temperature that can occur before an event is raised. The default is 55º Celsius.
Event severity when temperature exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the temperature exceeds the threshold. The default is 10.
Data Collection	
Collect data for temperature?	Select **Yes** to collect data about temperature for reports and graphs. The default is unselected.
Monitor Load	
Event Notification	
Raise event if load exceeds threshold?	Select **Yes** to raise an event if the UPS load exceeds the threshold that you set. The default is unselected.
Threshold - Maximum load	Specify the highest percentage of load that can occur before an event is raised. The default is 80%.
Event severity when load exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which load exceeds the threshold. The default is 10.
Data Collection	
Collect data for load?	Select **Yes** to collect data about load for reports and graphs. The default is unselected.
Monitor Output Voltage	
Event Notification	
Raise event if output voltage exceeds or falls below threshold?	Select **Yes** to raise an event if the output voltage level exceeds or falls below the thresholds that you set. The default is unselected.
Upper threshold	Select **Enable** to use an upper threshold value. The default is Enable.
Threshold - Maximum output voltage	Specify the highest output voltage that can occur before an event is raised. The default is 130 volts.
Event severity when output voltage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which output voltage exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is Enable.
Threshold - Minimum output voltage	Specify the lowest output voltage that can occur before an event is raised. The default is 100 volts.
Event severity when output voltage falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which output voltage falls below the threshold. The default is 10.
Data Collection	

Description	How To Set It
Collect data for output voltage?	Select **Yes** to collect data about output voltage for reports and graphs. The default is unselected.
Monitor Input Voltage	
Event Notification	
Raise event if input voltage exceeds or falls below threshold?	Select **Yes** to raise an event if the input voltage level exceeds or falls below the thresholds that you set. The default is unselected.
Upper threshold	Select **Enable** to use an upper threshold value. The default is Enable.
Threshold - Maximum input voltage	Specify the highest input voltage that can occur before an event is raised. The default is 130 volts.
Event severity when input voltage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which input voltage exceeds the threshold. The default is 10.
Lower threshold	Select **Enable** to use a lower threshold value. The default is Enable.
Threshold - Minimum input voltage	Specify the lowest input voltage that can occur before an event is raised. The default is 100 volts.
Event severity when input voltage falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which input voltage falls below the threshold. The default is 10.
Data Collection	
Collect data for input voltage?	Select **Yes** to collect data about input voltage for reports and graphs. The default is unselected.

Recommended Knowledge Script Group

The following Knowledge Scripts in the AppManager for Nortel BCMx module are members of the NortelBCMx recommended Knowledge Script Group (KSG).

- Alarms (Configure your Nortel BCM to send SNMP traps to AppManager before using this script. For more information, see "Identifying the SNMP Trap Receiver" on page 2904).
- ChassisUsage
- HealthCheck
- InterfaceHealth
- LogicalDiskSpace
- SystemUpTime
- SystemUsage

You can find the NortelBCMx KSG on the RECOMMENDED tab of the Knowledge Script pane of the Operator Console.

All the scripts in the KSG have their parameters set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab, and then run the NortelBCMx group on a Nortel BCMx resource.

Run the KSG from the Master view, not the NortelBCMx view. In order to use the Discovery_NortelBCMx Knowledge Script in a monitoring policy, the view must include root objects, which are not visible in the NortelBCMx view.

The NortelBCMx KSG enables a "best practices" usage of AppManager for monitoring your Nortel BCM environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView. For more information, see "About Policy-Based Monitoring" in the AppManager Help.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the NortelBCMx tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the NortelBCMx tab are not affected.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the NortelBCMx KSG and want to restore it to its original form, you can reinstall AppManager for Nortel BCMX on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\NortelBCMx` directory.

Discovery_NortelBCMx

Use this Knowledge Script to discover resource and configuration information for Nortel BCM software version 4.0 and hardware models 50, 50a, 50e, 200, 400, and 1000.

AppManager for Nortel BCMx provides limited support for Survivable Remote Gateway (SRG) mode and local mode with the Alarms, CallByCallLimits, ChassisUsage, HealthCheck, HuntGroupUsage, InterfaceHealth, LinkUtilization, PSTNFallback, SystemUpTime, and SystemUsage Knowledge Scripts. For more information, see the Help for those scripts.

Prerequisite

Configure your BCM user name and password into AppManager Security Manager. The discovery process will fail if it cannot access this vital information.

Resource Object

NT_MachineFolder

Default Schedule

By default, this script runs once a week on Sunday at 3 A.M.

Setting Parameter Values

Set the following parameters as needed.

Parameter	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the Discovery_NortelBCMx job fails. The default is 5.
Raise event if discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **Yes** to raise an event when the job succeeds. The default is unselected.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Raise event if discovery fails?	Select **Yes** to raise an event if discovery fails to find Nortel BCMx resources. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails to find Nortel BCMx resources. The default is 5.
Raise event if Nortel BCMx agent not installed?	Select **Yes** to raise an event if the Nortel BCMx managed object is not installed. The default is Yes.
Event severity when Nortel BCMx agent not installed	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the Nortel BCMx managed object is not installed. The default is 15.
Discover Nortel BCMx Devices	

Parameter	How To Set It
List of Nortel BCMx devices	Use this parameter if you have only a few Nortel BCM devices to discover. Type a list of the devices for which you want to discover resources. Use a comma to separate the names or IP addresses in the list. For example: `10.0.1.1,10.0.4.1`
List of Nortel BCMx device ranges	Use this parameter if you have only a few ranges of Nortel BCM devices to discover. Type a list of IP address ranges (up to 256 addresses) of the devices for which you want to discover resources. Only numbers, dashes, periods, and commas are allowed in the list. Use dashes to define a range. For example: `10.0.1.1-10.0.1.50,10.0.4.51-10.0.4.100`
Full path to file with list of Nortel BCMx devices	Instead of typing each Nortel BCM device separately, you can use this parameter to specify the full path to a file on the agent computer that contains a device name on each line of the file.

Chapter 50
NortelCC Knowledge Scripts

The NortelCC category provides the following Knowledge Scripts for monitoring Nortel Contact Center.

From the Knowledge Script view of Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AgentTimes	Monitors the total and percentage of time that Contact Center agents spend in various states.
Alarms	Monitors the Contact Center server for alarms (SNMP traps).
CallsAbandoned	Monitors various metrics related to abandoned calls.
CallsAnswered	Monitors various metrics related to answered calls.
CallsConfTrans	Monitors calls that have been conferenced in and out, and transferred in and out.
CallsOffered	Monitors the number of offered calls.
CallsTerminated	Monitors the number and percentage of terminated calls.
CallTimes	Monitors the amount of time calls spent in Contact Center before being transferred or receiving a type of call treatment.
CallTreatments	Monitors the number and percentage of calls that receive a type of call treatment.
Database	Monitors free space and used space for the Master, Blue, and Call-by-Call databases.
HealthCheck	Monitors the availability of services on the Contact Center server.
SkillsetTimes	Monitors the amount of time Contact Center skillsets spent in the following states: Active, All Agents Busy, and Staffed.
SystemUsage	Monitors Contact Center usage of system resources: CPU, memory, disk space, and network interfaces.

AgentTimes

Use this Knowledge Script to monitor the amount of time that Contact Center agents spend in the following states:

- Logged In Time
- Not Ready Time
- Talk Time
- Waiting Time

This script raises events if a value exceeds the threshold that you set. In addition, this script generates data streams for the percentage and total time spent in each state.

Not every data stream is generated for each resource object for which this script is valid. The following table provides a matrix for determining whether a data stream is generated for the resource object you are using.

	IVR Port Object	DNIS Object
Talk Time	Yes	Yes
Logged In Time	No	Yes
Not Ready Time	No	Yes
Waiting Time	No	Yes

The first time you run this script, it marks the time and date (a starting point) in the database. With subsequent iterations, the script monitors and collects data based on changes in the database since the last time the script ran.

Resource Objects

- NT_NORTELCC_IVRPORT
- NT_NORTELCC_DNIS

Default Schedule

By default, this script runs every 15 minutes. Because monitoring and data collection do not occur during the first iteration of this script, do not select the "Run Once" schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the AgentTimes job fails. The default is 5.
Raise event if SQL query fails?	Set to **Yes** to raise an event if the SQL query fails. The default is Yes. AppManager uses a SQL query to retrieve Contact Center database configuration information.

Parameter	How to Set It
Event severity when SQL query fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the SQL query fails to retrieve database configuration information. The default is 15.
Raise event if no new data is found?	Set to **Yes** to raise an event if the agent data has not changed since the last time the script ran. The default is Yes.
Event severity when no new data is found	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the agent data has not changed since the last time the script ran. The default is 15.
Monitor Total Logged In Time	
Data Collection	
Collect data for total Logged In time?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total amount of time agents were Logged In during the monitoring period. The default is unchecked.
Monitor Percentage of Time Logged In	
Event Notification	
Raise event if percentage of time Logged In falls below threshold?	Set to **Yes** to raise an event if the percentage of time that agents are Logged In falls below the threshold that you set. The default is Yes.
Threshold - Minimum percentage of time Logged In	Specify the minimum percentage of time that agents must be Logged In before an event is raised. The default is 100%.
Event severity when percentage of time Logged In exceeds threshold	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the percentage of time that agents are Logged In falls below the threshold you set. The default is 25.
Data Collection	
Collect data for percentage of time Logged In?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of time agents were Logged In during the monitoring period. The default is unchecked.
Monitor Total Not Ready Time	
Data Collection	
Collect data for total Not Ready time?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total amount of time agents were Not Ready during the monitoring period. The default is unchecked.
Monitor Percentage of Time Not Ready	
Event Notification	
Raise event if percentage of time Not Ready exceeds threshold?	Set to **Yes** to raise an event if the percentage of time that agents are Not Ready exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of time Not Ready	Specify the maximum percentage of time that agents must be Not Ready before an event is raised. The default is 70%.
Event severity when percentage of time Not Ready exceeds threshold	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the percentage of time that agents are Not Ready exceeds the threshold you set. The default is 25.
Data Collection	

Parameter	How to Set It
Collect data for percentage of time Not Ready?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of time agents were Not Ready during the monitoring period. The default is unchecked.
Monitor Total Talk Time	
Data Collection	
Collect data for total Talk time?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total amount of time agents were in Talk Time during the monitoring period. The default is unchecked.
Monitor Percentage of Time Talking	
Event Notification	
Raise event if percentage of time Talking exceeds threshold?	Set to **Yes** to raise an event if the percentage of time that agents are in Talk Time exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of time Talking	Specify the maximum percentage of time that agents must be in Talk Time before an event is raised. The default is 70%.
Event severity when percentage of time Talking exceeds threshold	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the percentage of time that agents are in Talk Time exceeds the threshold you set. The default is 25.
Data Collection	
Collect data for percentage of time Talking?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of time agents were in Talk Time during the monitoring period. The default is unchecked.
Monitor Total Time Waiting	
Data Collection	
Collect data for total Waiting time?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total amount of time agents were in Waiting Time during the monitoring period. The default is unchecked.
Monitor Percentage of Time Waiting	
Event Notification	
Raise event if percentage of time Waiting exceeds threshold?	Set to **Yes** to raise an event if the percentage of time that agents are in Waiting Time exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of time Waiting	Specify the maximum percentage of time that agents must be in Waiting Time before an event is raised. The default is 70%.
Event severity when percentage of time Waiting exceeds threshold	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the percentage of time that agents are in Waiting Time exceeds the threshold you set. The default is 25.
Data Collection	
Collect data for percentage of time Waiting?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of time agents were in Waiting Time during the monitoring period. The default is unchecked.

Alarms

Use this Knowledge Script to monitor the Contact Center server for alarms (SNMP traps): critical, major, minor, and indeterminate. This script raises events if any alarm is detected.

When setting parameters for this script, you will be asked to provide a list of alarm identifiers (system messages) that you want to include in or exclude from monitoring. Their format consists of a multi-letter mnemonic followed by a multi-digit alarm number, such as AUD000 or SRPT194. If you want to enter more than one alarm identifier, separate them with a comma as in the following example: `AUD000,SRPT194`.

If you choose to "Include only" selected alarm identifiers in a category, AppManager will generate events only for those identifiers. AppManager will not generate events for the other identifiers included in the category.

If you choose to "Exclude" selected alarm identifiers from a category, AppManager will generate events for all alarm identifiers included in the category except those that you specifically excluded.

If you accept the default parameter settings, which are "Exclude" and blank (in the *Alarm identifiers* parameter), AppManager will generate events for all identifiers in the category, because you excluded nothing from the category.

To allow this Knowledge Script to receive alarms from the Contact Center server, you need to configure the server's SNMP service.

Resource Object

NT_NORTELCC_SCCS

Default Schedule

By default, this script runs on an asynchronous schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Monitor critical alarms?	Set to **Yes** to monitor Contact Center for alarms in the critical category. The default is Yes.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers that you specify in the following parameter. • Select **Exclude** to exclude the listed identifiers from the critical category. • Select **Include only** to include *only* the listed identifiers in the critical category. By default, the critical category includes all alarms with critical severity in the SNMP trap.
Alarm identifiers	Type a comma-separated list of the alarm identifiers that you want to include in or exclude from the critical category. The default is an empty list.
Monitor major alarms?	Set to **Yes** to monitor Contact Center for alarms in the major category. The default is Yes.

Parameter	How to Set It
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers that you specify in the following parameter. • Select **Exclude** to exclude the listed identifiers from the major category. • Select **Include only** to include *only* the listed identifiers in the major category. By default, the critical category includes all alarms with major severity in the SNMP trap.
Alarm identifiers	Type a comma-separated list of the alarm identifiers that you want to include in or exclude from the major category. The default is an empty list.
Monitor minor alarms?	Set to **Yes** to monitor Contact Center for alarms in the minor category. The default is Yes.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers that you specify in the following parameter. • Select **Exclude** to exclude the listed identifiers from the minor category. • Select **Include only** to include *only* the listed identifiers in the minor category. By default, the critical category includes all alarms with minor severity in the SNMP trap.
Alarm identifiers	Type a comma-separated list of the alarm identifiers that you want to include in or exclude from the minor category. The default is an empty list.
Monitor indeterminate alarms?	Set to **Yes** to monitor Contact Center for alarms in the indeterminate category. The default is Yes.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers that you specify in the following parameter. • Select **Exclude** to exclude the listed identifiers from the indeterminate category. • Select **Include only** to include *only* the listed identifiers in the indeterminate category. By default, the critical category includes all alarms with indeterminate severity in the SNMP trap.
Alarm identifiers	Type a comma-separated list of the alarm identifiers that you want to include in or exclude from the indeterminate category. The default is an empty list.
Event Severities	
Severity - Critical alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a critical alarm is detected. The default is 10.
Severity - Major alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a major alarm is detected. The default is 15.
Severity - Minor alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a minor alarm is detected. The default is 20.
Severity - Indeterminate alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which an indeterminate alarm is detected. The default is 30.

CallsAbandoned

Use this Knowledge Script to monitor various metrics related to abandoned calls:

- Number and percentage of abandoned calls
- Number and percentage of calls abandoned after meeting or exceeding the delay threshold
- Total delay of abandoned calls
- Average and maximum delay of abandoned calls

This script raises an event if a value exceeds the threshold you set. In addition, this script generates data streams for each metric.

Not every data stream is generated for each resource object for which this script is valid. The following table is a matrix for determining whether a data stream is generated for the resource object you are using.

	CDN Object	DNIS Object	Application Object	AppSkillset Object
Calls Abandoned	Yes	Yes	Yes	Yes
% Calls Abandoned	Yes	Yes	Yes	Yes
Calls Abandoned After Threshold	No	Yes	Yes	Yes
% Calls Abandoned After Threshold	No	Yes	Yes	Yes
Calls Abandoned Delay	No	Yes	Yes	Yes
Maximum Abandoned Delay	No	Yes	Yes	Yes
Average Abandoned Delay	No	Yes	Yes	No

The first time you run this script, it marks the time and date (a starting point) in the database. With subsequent iterations, the script monitors and collects data based on changes in the database since the last time the script ran.

Resource Objects

- NT_NORTELCC_CDN
- NT_NORTELCC_DNIS
- NT_NORTELCC_APPLICATION
- NT_NORTELCC_APPSKILLSET

The TreeView pane of the Operator Console contains Application and Skillset objects under the NortelCC object. Within the Application and Skillset object folders are Application/Skillset (AppSkillset) pairs. The same pairs are represented within the Application and Skillset object folders. Their placement within the Application and Skillset folders allows you to search for a particular pair by either Application or Skillset. You can drop this Knowledge Script on a pair in either location.

Default Schedule

By default, this script runs every 15 minutes. Because monitoring and data collection do not occur during the first iteration of this script, do not select the “Run Once” schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallsAbandoned job fails. The default is 5.
Raise event if SQL query fails?	Set to **Yes** to raise an event if the SQL query fails. The default is Yes. AppManager uses a SQL query to retrieve Contact Center database configuration information.
Event severity when SQL query fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the SQL query fails to retrieve database configuration information. The default is 15.
Raise event if no new data is found?	Set to **Yes** to raise an event if the agent data has not changed since the last time the script ran. The default is Yes.
Event severity when no new data is found	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the agent data has not changed since the last time the script ran. The default is 15.
Monitor Calls Abandoned	
Data Collection	
Collect data for calls abandoned?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls that were abandoned during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Abandoned	
Event Notification	
Raise event if percentage of calls abandoned exceeds threshold?	Set to **Yes** to raise an event if the percentage of abandoned calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls abandoned	Specify the maximum percentage of calls that must be abandoned before an event is raised. The default is 90%.
Event severity when percentage of calls abandoned exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of abandoned calls exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls abandoned?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that were abandoned during the monitoring period. The default is unchecked.
Monitor Calls Abandoned After Meeting or Exceeding Delay Ceiling	
Data Collection	
Collect data for calls abandoned after meeting or exceeding delay ceiling?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls that were abandoned during the monitoring period after meeting or exceeding the delay ceiling. The default is unchecked.
Monitor Percentage of Calls Abandoned After Meeting or Exceeding Delay Ceiling	

Parameter	How to Set It
Event Notification	
Raise event if percentage of calls abandoned after meeting or exceeding delay ceiling exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that were abandoned after meeting or exceeding the delay ceiling exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls abandoned after meeting or exceeding delay ceiling	Specify the maximum percentage of calls that can be abandoned after meeting or exceeding the delay ceiling before an event is raised. The default is 70%.
Event severity when percentage of calls abandoned after meeting or exceeding delay ceiling exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that were abandoned after meeting or exceeding the delay ceiling exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls abandoned after meeting or exceeding delay ceiling?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that were abandoned during the monitoring period after meeting or exceeding the delay ceiling. The default is unchecked.
Monitor Total Delay of Calls Abandoned	
Data Collection	
Collect data for total delay of calls abandoned?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total amount of delay experienced by abandoned calls during the monitoring period. The default is unchecked.
Monitor Average Abandoned Delay	
Event Notification	
Raise event if average abandoned delay exceeds threshold?	Set to **Yes** to raise an event if the average amount of delay experienced by abandoned calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum average abandoned delay	Specify the maximum average amount of delay that abandoned calls can experience before an event is raised. The default is 10 seconds.
Event severity when average abandoned delay exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average amount of delay experienced by abandoned calls exceeds the threshold. The default is 25.
Data Collection	
Collect data for average abandoned delay?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the average amount of delay that occurred during the monitoring period. The default is unchecked.
Monitor Maximum Abandoned Delay	
Event Notification	
Raise event if maximum abandoned delay exceeds threshold?	Set to **Yes** to raise an event if the maximum amount of delay experienced by abandoned calls exceeds the threshold that you set. The default is Yes.
Threshold - Highest maximum abandoned delay	Specify the highest amount of maximum delay that abandoned calls can experience before an event is raised. The default is 10 seconds.

Parameter	How to Set It
Event severity when maximum abandoned delay exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average amount of delay experienced by abandoned calls exceeds the threshold. The default is 25.
Data Collection	
Collect data for maximum abandoned delay?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the maximum amount of delay experienced by abandoned calls during the monitoring period. The default is unchecked.

CallsAnswered

Use this Knowledge Script to monitor various metrics related to answered calls:

- Number and percentage of answered calls
- Number and percentage of calls answered after meeting or exceeding the delay threshold
- Total delay of answered calls
- Average and maximum delay of answered calls
- Total delay of calls answered at skillset
- Average and maximum delay of calls answered at skillset

This script raises an event if a value exceeds the threshold you set. In addition, this script generates data streams for each metric.

Not every data stream is generated for each resource object for which this script is valid. The following table is a matrix for determining whether a data stream is generated for the resource object you are using.

	CDN Object	DNIS Object	IVRQueue Object	IVRPort Object	Application Object	AppSkillset Object
Calls Answered	Yes	Yes	Yes	Yes	Yes	Yes
% Calls Answered	Yes	Yes	Yes	No	Yes	Yes
Calls Answered After Threshold	No	Yes	Yes	No	Yes	Yes
% Calls Answered After Threshold	No	Yes	Yes	No	Yes	Yes
Calls Answered Delay	No	Yes	Yes	No	Yes	Yes
Maximum Answered Delay	No	Yes	No	No	Yes	Yes
Average Answered Delay	No	Yes	Yes	No	Yes	Yes
Calls Answered Delay at Skillset	No	No	No	No	Yes	Yes
Maximum Answered Delay at Skillset	No	No	No	No	Yes	Yes
Average Answered Delay at Skillset	No	No	No	No	Yes	Yes

When dropped on a proper resource object, AppManager generates data streams as noted in the table.

The first time you run this script, it marks the time and date (a starting point) in the database. With subsequent iterations, the script monitors and collects data based on changes in the database since the last time the script ran.

Resource Objects

- NT_NORTELCC_CDN
- NT_NORTELCC_DNIS
- NT_NORTELCC_IVRQUEUE
- NT_NORTELCC_IVRPORT
- NT_NORTELCC_APPLICATION

- NT_NORTELCC_APPSKILLSET
  The TreeView pane of the Operator Console contains Application and Skillset objects under the NortelCC object. Within the Application and Skillset object folders are Application/Skillset (AppSkillset) pairs. The same pairs are represented within the Application and Skillset object folders. Their placement within the Application and Skillset folders allows you to search for a particular pair by either Application or Skillset. You can drop this Knowledge Script on a pair in either location.

Default Schedule

By default, this script runs every 15 minutes. Because monitoring and data collection do not occur during the first iteration of this script, do not select the "Run Once" schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallsAnswered job fails. The default is 5.
Raise event if SQL query fails?	Set to **Yes** to raise an event if the SQL query fails. The default is Yes. AppManager uses a SQL query to retrieve Contact Center database configuration information.
Event severity when SQL query fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the SQL query fails to retrieve database configuration information. The default is 15.
Raise event if no new data is found?	Set to **Yes** to raise an event if the agent data has not changed since the last time the script ran. The default is Yes.
Event severity when no new data is found	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the agent data has not changed since the last time the script ran. The default is 15.
Monitor Calls Answered	
Data Collection	
Collect data for calls answered?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls that were answered during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Answered	
Event Notification	
Raise event if percentage of calls answered falls below threshold?	Set to **Yes** to raise an event if the percentage of answered calls falls below the threshold that you set. The default is Yes. **Important** If you drop this script on a resource object that is not configured to answer calls, AppManager raises an event indicating that the percentage of answered calls for that object has indeed fallen below the threshold. The threshold is 90%. An object that is not configured to answer calls will have 0% answered calls — a value well below the threshold. To prevent this sort of invalid event, drop this script on a resource object that *is* configured to answer calls.

Parameter	How to Set It
Threshold - Minimum percentage of calls answered	Specify the minimum percentage of calls that can be answered to prevent an event from being raised. The default is 90%.
Event severity when percentage of calls answered falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of answered calls falls below the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls answered?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that were answered during the monitoring period. The default is unchecked.
Monitor Calls Answered After Meeting or Exceeding Delay Ceiling	
Data Collection	
Collect data for calls answered after meeting or exceeding delay ceiling?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls that were answered during the monitoring period after meeting or exceeding the delay ceiling. The default is unchecked.
Monitor Percentage of Calls Answered After Meeting or Exceeding Delay Ceiling	
Event Notification	
Raise event if percentage of calls answered after meeting or exceeding delay ceiling exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that were answered after meeting or exceeding the delay ceiling exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls answered after meeting or exceeding delay ceiling	Specify the maximum percentage of calls that can be answered after meeting or exceeding the delay ceiling before an event is raised. The default is 70%.
Event severity when percentage of calls answered after meeting or exceeding delay ceiling exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that were answered after meeting or exceeding the delay ceiling exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls answered after meeting or exceeding delay ceiling?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that were answered during the monitoring period after meeting or exceeding the delay ceiling. The default is unchecked.
Monitor Total Delay of Calls Answered	
Data Collection	
Collect data for total delay of calls answered?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total amount of delay experienced by answered calls during the monitoring period. The default is unchecked.
Monitor Average Answered Delay	
Event Notification	
Raise event if average answered delay exceeds threshold?	Set to **Yes** to raise an event if the average amount of delay experienced by answered calls exceeds the threshold that you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum average answered delay	Specify the maximum average amount of delay that answered calls can experience before an event is raised. The default is 10 seconds.
Event severity when average answered delay exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average amount of delay experienced by answered calls exceeds the threshold. The default is 25.
Data Collection	
Collect data for average answered delay?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the average amount of delay that occurred during the monitoring period. The default is unchecked.
Monitor Maximum Answered Delay	
Event Notification	
Raise event if maximum answered delay exceeds threshold?	Set to **Yes** to raise an event if the maximum amount of delay experienced by answered calls exceeds the threshold that you set. The default is Yes.
Threshold - Highest maximum answered delay	Specify the highest amount of maximum delay that answered calls can experience before an event is raised. The default is 10 seconds.
Event severity when maximum answered delay exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average amount of delay experienced by answered calls exceeds the threshold. The default is 25.
Data Collection	
Collect data for maximum answered delay?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the maximum amount of delay experienced by answered calls during the monitoring period. The default is unchecked.
Monitor Total Answered Delay at Skillset	
Data Collection	
Collect data for total answered delay at skillset?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total amount of delay experienced by calls answered by a particular skillset during the monitoring period. The default is unchecked.
Monitor Average Answered Delay at Skillset	
Event Notification	
Raise event if average answered delay at skillset exceeds threshold?	Set to **Yes** to raise an event if the average amount of delay experienced by calls answered by a particular skillset exceeds the threshold that you set. The default is Yes.
Threshold - Maximum average answered delay at skillset	Specify the maximum average amount of delay that answered calls can experience at a particular skillset before an event is raised. The default is 10 seconds.
Event severity when average answered delay at skillset exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the average amount of delay experienced by calls answered by a particular skillset exceeds the threshold. The default is 25.
Data Collection	
Collect data for average answered delay at skillset?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the average amount of delay experienced by calls answered by a particular skillset during the monitoring period. The default is unchecked.
Monitor Maximum Answered Delay at Skillset	
Event Notification	

Parameter	How to Set It
Raise event if maximum answered delay at skillset exceeds threshold?	Set to **Yes** to raise an event if the maximum amount of delay experienced by calls answered by a particular skillset exceeds the threshold that you set. The default is Yes.
Threshold - Highest maximum answered delay at skillset	Specify the highest amount of maximum delay that answered calls can experience at a particular skillset before an event is raised. The default is 10 seconds.
Event severity when maximum answered delay at skillset exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the maximum amount of delay experienced by calls answered by a particular skillset exceeds the threshold. The default is 25.
Data Collection	
Collect data for maximum answered delay at skillset?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the maximum amount of delay experienced by calls answered by a particular skillset during the monitoring period. The default is unchecked.

CallsConfTrans

Use this Knowledge Script to monitor calls that are transferred in and out of Contact Center, and to monitor calls that have been conferenced in and out of Contact Center. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for each metric.

Not every data stream is generated for each resource object for which this script is valid. The following table is a matrix for determining whether a data stream is generated for the resource object you are using.

	IVRQueue Object	IVRPort Object	Application Object
Calls Conferenced Out	Yes	Yes	Yes
Calls Conferenced In	No	No	Yes
% Calls Conferenced Out	Yes	Yes	Yes
% Calls Conferenced In	No	No	Yes
Calls Transferred Out	Yes	Yes	Yes
Calls Transferred In	No	No	Yes
% Calls Transferred Out	Yes	Yes	Yes
% Calls Transferred In	No	No	Yes

The first time you run this script, it marks the time and date (a starting point) in the database. With subsequent iterations, the script monitors and collects data based on changes in the database since the last time the script ran.

Resource Objects

- NT_NORTELCC_IVRQUEUE
- NT_NORTELCC_IVRPORT
- NT_NORTELCC_APPLICATION

Default Schedule

By default, this script runs every 15 minutes. Because monitoring and data collection do not occur during the first iteration of this script, do not select the "Run Once" schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallsConfTrans job fails. The default is 5.
Raise event if SQL query fails?	Set to **Yes** to raise an event if the SQL query fails. The default is Yes. AppManager uses a SQL query to retrieve Contact Center database configuration information.

Parameter	How to Set It
Event severity when SQL query fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the SQL query fails to retrieve database configuration information. The default is 15.
Raise event if no new data is found?	Set to **Yes** to raise an event if the agent data has not changed since the last time the script ran. The default is Yes.
Event severity when no new data is found	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the agent data has not changed since the last time the script ran. The default is 15.
Monitor Calls Conferenced In	
Data Collection	
Collect data for calls answered?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls that were conferenced in during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Conferenced In	
Event Notification	
Raise event if percentage of calls conferenced in exceeds threshold?	Set to **Yes** to raise an event if the percentage of conferenced-in calls exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls conferenced in	Specify the maximum percentage of calls that must be conferenced in before an event is raised. The default is 0%.
Event severity when percentage of calls conferenced in exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of conferenced-in calls exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls conferenced in?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that were conferenced in during the monitoring period. The default is unchecked.
Monitor Calls Conferenced Out	
Data Collection	
Collect data for calls conferenced out?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls that were conferenced out during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Conferenced Out	
Event Notification	
Raise event if percentage of calls conferenced out exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that were conferenced out exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls conferenced out	Specify the maximum percentage of calls that can be conferenced out before an event is raised. The default is 0%.
Event severity when percentage of calls conferenced out exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of conferenced-out calls exceeds the threshold. The default is 25.
Data Collection	

Parameter	How to Set It
Collect data for percentage of calls conferenced out?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that were conferenced out during the monitoring period. The default is unchecked.
Monitor Calls Transferred In	
Data Collection	
Collect data for calls transferred in?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls that were transferred in during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Transferred In	
Event Notification	
Raise event if percentage of calls transferred in exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that were transferred in exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls transferred in	Specify the maximum percentage of calls that must be transferred in before an event is raised. The default is 0%.
Event severity when percentage of calls transferred in exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of transferred-in calls exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls transferred in?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls transferred in during the monitoring period. The default is unchecked.
Monitor Calls Transferred Out	
Data Collection	
Collect data for calls transferred out?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of calls transferred out during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Transferred Out	
Event Notification	
Raise event if percentage of calls transferred out exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls transferred out exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls transferred out	Specify the maximum percentage of calls that must be transferred out before an event is raised. The default is 0 calls.
Event severity when percentage of calls transferred out exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of transferred-out calls exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls transferred out?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls transferred out during the monitoring period. The default is unchecked.

CallsOffered

Use this Knowledge Script to monitor the number of calls that have been offered to Contact Center. This script generates data streams for the number of offered calls per resource object.

The first time you run this script, it marks the time and date (a starting point) in the database. With subsequent iterations, the script monitors and collects data based on changes in the database since the last time the script ran.

Resource Objects

- NT_NORTELCC_CDN
- NT_NORTELCC_DNIS
- NT_NORTELCC_IVRQUEUE
- NT_NORTELCC_APPLICATION
- NT_NORTELCC_APPSKILLSET

Default Schedule

By default, this script runs every 15 minutes. Because monitoring and data collection do not occur during the first iteration of this script, do not select the "Run Once" schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallsOffered job fails. The default is 5.
Raise event if SQL query fails?	Set to **Yes** to raise an event if the SQL query fails. The default is Yes. AppManager uses a SQL query to retrieve Contact Center database configuration information.
Event severity when SQL query fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the SQL query fails to retrieve database configuration information. The default is 15.
Raise event if no new data is found?	Set to **Yes** to raise an event if the agent data has not changed since the last time the script ran. The default is Yes.
Event severity when no new data is found	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the agent data has not changed since the last time the script ran. The default is 15.
Monitor Calls Offered	
Data Collection	
Collect data for calls offered?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls that were offered to Contact Center during the monitoring period. The default is unchecked.

CallsTerminated

Use this Knowledge Script to monitor the number and percentage of terminated calls. This script raises an event if the percentage of terminated calls falls below the threshold that you set. In addition, this script generates data streams for the number and percentage of terminated calls.

The first time you run this script, it marks the time and date (a starting point) in the database. With subsequent iterations, the script monitors and collects data based on changes in the database since the last time the script ran.

Resource Object

NT_NORTELCC_CDN

Default Schedule

By default, this script runs every 15 minutes. Because monitoring and data collection do not occur during the first iteration of this script, do not select the "Run Once" schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallsTerminated job fails. The default is 5.
Raise event if SQL query fails?	Set to **Yes** to raise an event if the SQL query fails. The default is Yes. AppManager uses a SQL query to retrieve Contact Center database configuration information.
Event severity when SQL query fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the SQL query fails to retrieve database configuration information. The default is 15.
Raise event if no new data is found?	Set to **Yes** to raise an event if the agent data has not changed since the last time the script ran. The default is Yes.
Event severity when no new data is found	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the agent data has not changed since the last time the script ran. The default is 15.
Monitor Calls Terminated	
Data Collection	
Collect data for calls terminated?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls that were terminated during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Terminated	
Event Notification	

Parameter	How to Set It
Raise event if percentage of calls terminated falls below threshold?	Set to **Yes** to raise an event if the percentage of terminated calls falls below the threshold that you set. The default is Yes.
Threshold - Minimum percentage of calls terminated	Specify the minimum percentage of calls that must be terminated before an event is raised. The default is 90%.
Event severity when percentage of calls terminated falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of terminated calls falls below the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls terminated?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that were terminated during the monitoring period. The default is unchecked.

CallTimes

Use this Knowledge Script to monitor the time that calls spend in Contact Center before being transferred or receiving a type of call treatment. This script raises an event if a value exceeds a threshold that you set. In addition, this script generates the following data streams:

- TimeBeforeDefault
- TimeBeforeForceBusy
- TimeBeforeForceDisconnect
- TimeBeforeForceOverflow
- TimeBeforeInterflow
- TimeBeforeIVRTransfer
- TimeBeforeRouteTo
- AvgTimeBeforeDefault
- AvgTimeBeforeForceBusy
- AvgTimeBeforeForceDisconnect
- AvgTimeBeforeForceOverflow
- AvgTimeBeforeInterflow
- AvgTimeBeforeRouteTo

The first time you run this script, it marks the time and date (a starting point) in the database. With subsequent iterations, the script monitors and collects data based on changes in the database since the last time the script ran.

Resource Object

NT_NORTELCC_APPLICATION

Default Schedule

By default, this script runs every 15 minutes. Because monitoring and data collection do not occur during the first iteration of this script, do not select the "Run Once" schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallTimes job fails. The default is 5.
Raise event if SQL query fails?	Set to **Yes** to raise an event if the SQL query fails. The default is Yes. AppManager uses a SQL query to retrieve Contact Center database configuration information.

Parameter	How to Set It
Event severity when SQL query fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the SQL query fails to retrieve database configuration information. The default is 15.
Raise event if no new data is found?	Set to **Yes** to raise an event if the agent data has not changed since the last time the script ran. The default is Yes.
Event severity when no new data is found	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the agent data has not changed since the last time the script ran. The default is 15.
Monitor Total Time Calls Spent in System Before Default Treatment	
Data Collection	
Collect data for total time calls spent in system before default treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of seconds that calls spent in Contact Center before receiving the default treatment. The default is unchecked.
Monitor Average Time Calls Spent in System Before Default Treatment	
Event Notification	
Raise event if average time calls spent in system before default treatment exceeds threshold?	Set to **Yes** to raise an event if the average time that calls spent in Contact Center before receiving the default treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum average time calls spent in system before default treatment	Specify the highest average time that calls can spend in Contact Center (before receiving the default treatment) before an event is raised. The default is 10 seconds.
Event severity when average time calls spent in system before default treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the highest average time that calls spent in Contact Center (before receiving the default treatment) exceeds the threshold. The default is 25.
Data Collection	
Collect data for average time calls spent in system before default treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the highest average time that calls spent in Contact Center during the monitoring period before receiving the default treatment. The default is unchecked.
Monitor Total Time Calls Spent in System Before Force Busy Treatment	
Data Collection	
Collect data for total time calls spent in system before force busy treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of seconds that calls spent in Contact Center before receiving the force busy treatment. The default is unchecked.
Monitor Average Time Calls Spent in System Before Force Busy Treatment	
Event Notification	
Raise event if average time calls spent in system before force busy treatment exceeds threshold?	Set to **Yes** to raise an event if the average time that calls spent in Contact Center before receiving the force busy treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum average time calls spent in system before force busy treatment	Specify the highest average time that calls can spend in Contact Center (before receiving the force busy treatment) before an event is raised. The default is 10 seconds.

Parameter	How to Set It
Event severity when average time calls spent in system before force busy treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the highest average time that calls spent in Contact Center (before receiving the force busy treatment) exceeds the threshold. The default is 25.
Data Collection	
Collect data for average time calls spent in system before force busy treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the highest average time that calls spent in Contact Center during the monitoring period before receiving the force busy treatment. The default is unchecked.
Monitor Total Time Calls Spent in System Before Disconnect Treatment	
Data Collection	
Collect data for total time calls spent in system before disconnect treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of seconds that calls spent in Contact Center before receiving the disconnect treatment. The default is unchecked.
Monitor Average Time Calls Spent in System Before Disconnect Treatment	
Event Notification	
Raise event if average time calls spent in system before disconnect treatment exceeds threshold?	Set to **Yes** to raise an event if the average time that calls spent in Contact Center before receiving the disconnect treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum average time calls spent in system before disconnect treatment	Specify the highest average time that calls can spend in Contact Center (before receiving the disconnect treatment) before an event is raised. The default is 10 seconds.
Event severity when average time calls spent in system before disconnect treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the highest average time that calls spent in Contact Center (before receiving the disconnect treatment) exceeds the threshold. The default is 25.
Data Collection	
Collect data for average time calls spent in system before disconnect treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the highest average time that calls spent in Contact Center during the monitoring period before receiving the disconnect treatment. The default is unchecked.
Monitor Total Time Calls Spent in System Before Force Overflow Treatment	
Data Collection	
Collect data for total time calls spent in system before force overflow treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of seconds that calls spent in Contact Center before receiving the force overflow treatment. The default is unchecked.
Monitor Average Time Calls Spent in System Before Force Overflow Treatment	
Event Notification	
Raise event if average time calls spent in system before force overflow treatment exceeds threshold?	Set to **Yes** to raise an event if the average time that calls spent in Contact Center before receiving the force overflow treatment exceeds the threshold that you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum average time calls spent in system before force overflow treatment	Specify the highest average time that calls can spend in Contact Center (before receiving the force overflow treatment) before an event is raised. The default is 10 seconds.
Event severity when average time calls spent in system before force overflow treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the highest average time that calls spent in Contact Center (before receiving the force overflow treatment) exceeds the threshold. The default is 25.
Data Collection	
Collect data for average time calls spent in system before force overflow treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the highest average time that calls spent in Contact Center during the monitoring period before receiving the force overflow treatment. The default is unchecked.
Monitor Total Time Calls Spent in Master_Script	
Data Collection	
Collect data for total time calls spent in Master_Script?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of seconds that calls spent in Master_Script. The default is unchecked.
Monitor Average Time Calls Spent in Master_Script	
Event Notification	
Raise event if average time calls spent in Master_Script exceeds threshold?	Set to **Yes** to raise an event if the average time that calls spent in Master_Script exceeds the threshold that you set. The default is Yes.
Threshold - Maximum average time calls spent in Master_Script	Specify the highest average time that calls can spend in Master_Script before an event is raised. The default is 10 seconds.
Event severity when average time calls spent in Master_Script exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the highest average time that calls spent in Master_Script exceeds the threshold. The default is 25.
Data Collection	
Collect data for average time calls spent in Master_Script?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the highest average time that calls spent in Master_Script. The default is unchecked.
Monitor Total Time Calls Spent in System Before Transfer to IVR	
Data Collection	
Collect data for total time calls spent in system before transfer to IVR?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of seconds that calls spent in Contact Center before being transferred to an Interactive Voice Response (IVR) system. The default is unchecked.
Monitor Total Time Calls Spent in System Before Route Call Treatment	
Data Collection	
Collect data for total time calls spent in system before route call treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of seconds that calls spent in Contact Center before receiving route call treatment. The default is unchecked.
Monitor Average Time Calls Spent in System Before Route Call Treatment	

Parameter	How to Set It
Event Notification	
Raise event if average time calls spent in system before route call treatment exceeds threshold?	Set to **Yes** to raise an event if the average time that calls spent in Contact Center before receiving route call treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum average time calls spent in system before route call treatment	Specify the highest average time that calls can spend in Contact Center (before receiving route call treatment) before an event is raised. The default is 10 seconds.
Event severity when average time calls spent in system before route call treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the highest average time that calls spent in Contact Center (before receiving route call treatment) exceeds the threshold. The default is 25.
Data Collection	
Collect data for average time calls spent in system before route call treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the highest average time that calls spent in Contact Center before receiving route call treatment. The default is unchecked.

CallTreatments

Use this Knowledge Script to monitor the number and percentage of calls that receive several types of call treatments:

- Broadcast
- Default
- Force Busy
- Force Disconnect
- Force Overflow
- Host Lookup
- IVR
- Music
- RAN
- Route Call

This script raises an event if a threshold is exceeded. In addition, this script generates data streams for each metric.

Not every data stream is generated for each resource object for which this script is valid. The following table is a matrix for determining whether a data stream is generated for the resource object you are using.

	DNIS Object	Application Object
Calls Given Broadcast	No	Yes
% Calls Given Broadcast	No	Yes
Calls Given Default	Yes	Yes
% Calls Given Default	Yes	Yes
Calls Given Force Busy	Yes	Yes
% Calls Given Force Busy	Yes	Yes
Calls Given Force Disconnect	Yes	Yes
% Calls Given Force Disconnect	Yes	Yes
Calls Given Force Overflow	Yes	Yes
% Calls Given Force Overflow	Yes	Yes
Calls Given Host Lookup	No	Yes
% Calls Given Host Lookup	No	Yes
Calls Given IVR	No	Yes
% Calls Given IVR	No	Yes
Calls Given Music	No	Yes
% Calls Given Music	No	Yes
Calls Given RAN	No	Yes
% Calls Given RAN	No	Yes
Calls Given Route Call	Yes	Yes
% Calls Given Route Call	Yes	Yes

The first time you run this script, it marks the time and date (a starting point) in the database. With subsequent iterations, the script monitors and collects data based on changes in the database since the last time the script ran.

Resource Objects

- NT_NORTELCC_DNIS
- NT_NORTELCC_APPLICATION

Default Schedule

By default, this script runs every 15 minutes. Because monitoring and data collection do not occur during the first iteration of this script, do not select the "Run Once" schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallTreatments job fails. The default is 5.
Raise event if SQL query fails?	Set to **Yes** to raise an event if the SQL query fails. The default is Yes. AppManager uses a SQL query to retrieve Contact Center database configuration information.
Event severity when SQL query fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the SQL query fails to retrieve database configuration information. The default is 15.
Raise event if no new data is found?	Set to **Yes** to raise an event if the agent data has not changed since the last time the script ran. The default is Yes.
Event severity when no new data is found	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the agent data has not changed since the last time the script ran. The default is 15.
Monitor Calls Given Broadcast Treatment	
Data Collection	
Collect data for calls given broadcast treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls that received broadcast treatment during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Given Broadcast Treatment	
Event Notification	
Raise event if percentage of calls given broadcast treatment exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that received broadcast treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls given broadcast treatment	Specify the maximum percentage of calls that must receive broadcast treatment before an event is raised. The default is 70%.

Parameter	How to Set It
Event severity when percentage of calls given broadcast treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that received broadcast treatment exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls given broadcast treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that received broadcast treatment during the monitoring period. The default is unchecked.
Monitor Calls Given Default Treatment	
Data Collection	
Collect data for calls given default treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls that received default treatment during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Given Default Treatment	
Event Notification	
Raise event if percentage of calls given default treatment exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that received default treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls given default treatment	Specify the maximum percentage of calls that can receive default treatment before an event is raised. The default is 70%.
Event severity when percentage of calls given default treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that received default treatment exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls given default treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that received default treatment during the monitoring period. The default is unchecked.
Monitor Calls Given Force Busy Treatment	
Data Collection	
Collect data for calls given force busy treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of calls that received force busy treatment during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Given Force Busy Treatment	
Event Notification	
Raise event if percentage of calls given force busy treatment exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that received force busy treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls given force busy treatment	Specify the maximum percentage of calls that can receive force busy treatment before an event is raised. The default is 70%.

Parameter	How to Set It
Event severity when percentage of calls given force busy treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that received force busy treatment exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls given force busy treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that received force busy treatment during the monitoring period. The default is unchecked.
Monitor Calls Given Force Disconnect Treatment	
Data Collection	
Collect data for calls given force disconnect treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of calls that received force disconnect treatment during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Given Force Disconnect Treatment	
Event Notification	
Raise event if percentage of calls given force disconnect treatment exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that received force disconnect treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls given force disconnect treatment	Specify the maximum percentage of calls that can receive force disconnect treatment before an event is raised. The default is 70%.
Event severity when percentage of calls given force disconnect treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that received force disconnect treatment exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls given force disconnect treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that received force disconnect treatment during the monitoring period. The default is unchecked.
Monitor Calls Given Force Overflow Treatment	
Data Collection	
Collect data for calls given force overflow treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of calls that received force overflow treatment during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Given Force Overflow Treatment	
Event Notification	
Raise event if percentage of calls given force overflow treatment exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that received force overflow treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls given force overflow treatment	Specify the maximum percentage of calls that can receive force overflow treatment before an event is raised. The default is 70%.

Parameter	How to Set It
Event severity when percentage of calls given force overflow treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that received force overflow treatment exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls given force overflow treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that received force overflow treatment during the monitoring period. The default is unchecked.
Monitor Calls Given Host Lookup Treatment	
Data Collection	
Collect data for calls given host lookup treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of calls that received host lookup treatment during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Given Host Lookup Treatment	
Event Notification	
Raise event if percentage of calls given host lookup treatment exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that received host lookup treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls given host lookup treatment	Specify the maximum percentage of calls that can receive host lookup treatment before an event is raised. The default is 70%.
Event severity when percentage of calls given host lookup treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that received host lookup treatment exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls given host lookup treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that received host lookup treatment during the monitoring period. The default is unchecked.
Monitor Calls Given IVR Treatment	
Data Collection	
Collect data for calls given IVR treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of calls that received IVR treatment during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Given IVR Treatment	
Event Notification	
Raise event if percentage of calls given IVR treatment exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that received IVR treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls given IVR treatment	Specify the maximum percentage of calls that can receive IVR treatment before an event is raised. The default is 70%.

Parameter	How to Set It
Event severity when percentage of calls given IVR treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that received IVR treatment exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls given IVR treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that received IVR treatment during the monitoring period. The default is unchecked.
Monitor Calls Given Music Treatment	
Data Collection	
Collect data for calls given music treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of calls that received music treatment during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Given Music Treatment	
Event Notification	
Raise event if percentage of calls given music treatment exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that received music treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls given music treatment	Specify the maximum percentage of calls that can receive music treatment before an event is raised. The default is 70%.
Event severity when percentage of calls given music treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that received music treatment exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls given music treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that received music treatment during the monitoring period. The default is unchecked.
Monitor Calls Given RAN Treatment	
Data Collection	
Collect data for calls given RAN treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of calls that received a recorded announcement during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Given RAN Treatment	
Event Notification	
Raise event if percentage of calls given RAN treatment exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that received a recorded announcement exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls given RAN treatment	Specify the maximum percentage of calls that can receive a recorded announcement before an event is raised. The default is 70%.

Parameter	How to Set It
Event severity when percentage of calls given RAN treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that received a recorded announcement exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls given RAN treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that received a recorded announcement during the monitoring period. The default is unchecked.
Monitor Calls Given Route Call Treatment	
Data Collection	
Collect data for calls given route call treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total number of calls that received route call treatment during the monitoring period. The default is unchecked.
Monitor Percentage of Calls Given Route Call Treatment	
Event Notification	
Raise event if percentage of calls given route call treatment exceeds threshold?	Set to **Yes** to raise an event if the percentage of calls that received route call treatment exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of calls given route call treatment	Specify the maximum percentage of calls that can receive route call treatment before an event is raised. The default is 70%.
Event severity when percentage of calls given route call treatment exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of calls that received route call treatment exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage of calls given route call treatment?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of calls that received route call treatment during the monitoring period. The default is unchecked.

Database

Use this Knowledge Script to monitor free and used space in the Master, Blue, and Call-by-Call databases. This script raises an event if a value exceeds or falls below a threshold. In addition, this script generates data streams for the following metrics:

- Total free space
- Percentage of used space

Resource Object

NT_NORTELCC_DATABASE

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Database job fails. The default is 5.
Raise event if SQL query fails?	Set to **Yes** to raise an event if the SQL query fails. The default is Yes. AppManager uses a SQL query to retrieve Contact Center database configuration information.
Event severity when SQL query fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the SQL query fails to retrieve database configuration information. The default is 15.
Raise event if no new data is found?	Set to **Yes** to raise an event if database data has not changed since the last time the script ran. The default is Yes.
Event severity when no new data is found	Set the event severity level, from 1 to 40, to reflect the importance of an event in which database data has not changed since the last time the script ran. The default is 15.
Monitor Free Space	
Data Collection	
Collect data for free space?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the total amount of free disk space on the databases. The default is unchecked.
Monitor Percentage Used Space	
Event Notification	
Raise event if percentage used space exceeds threshold?	Set to **Yes** to raise an event if the percentage of used disk space exceeds the threshold that you set. The default is Yes.

Parameter	How to Set It
Threshold - Maximum percentage used space	Specify the maximum percentage of disk space that can be used before an event is raised. The default is 90%.
Event severity when percentage used space exceeds threshold.	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of used disk space exceeds the threshold. The default is 25.
Data Collection	
Collect data for percentage used space?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of used disk space for the databases. The default is unchecked.

HealthCheck

Use this Knowledge Script to monitor the availability of services on the Contact Center server. This script raises an event if a service is unavailable. In addition, this script can generate data streams for service availability.

This script can monitor the services listed in the following table. All but two, Host Application Integration and TAO NT Naming Service, are monitored by default. Nortel does not consider these two services to be critical. You should refer to your Nortel Symposium Call Center documentation to determine the relevancy of the other monitored services in your Contact Center environment.

Use the *Services to monitor* parameters to select and deselect services as appropriate for your installation of Contact Center. If your initial selection does not suit your needs, simply rerun this script until you are monitoring an ideal combination of services.

AUDIT_Service	DBNotifier_Service	EB_Service
ES_Service	HDC_Service	HDM_Service
Host Application Integration	IceEmHlpService	IceRTDService
IS_Service	MAS Backup/Restore	MAS Configuration Manager
MAS Event Scheduler	MAS Fault Manager	MAS LinkHandler Port #2
MAS OM Server	MAS Security	MAS Service Daemon
MAS Service Manager	MAS Time Service	MLSM_Service
NBNM_Service	NBTSM_Service	NCCOAM_Service
NDLOAM_Service	NITSM_Service	OAM_Service
pcAnywhere Host Service	RDC_Service	RSM_Service
SDMCA_Service	SDP_Service	Sybase BCKServer
Sybase MONServer	Sybase SQLServer	Sybase XPServer
SymposiumWC	TAO NT Naming Service	TFA_Service
TFABridge_Service	TFE_Service	VSM_Service

Resource Object

NortelCC_SCCS

Default Schedule

By default, this script runs every minute.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the HealthCheck job fails. The default is 5.

Parameter	How to Set It
Raise event if a service is not found?	Set to **Yes** to raise an event if a monitored service cannot be found on the Contact Center server. The default is Yes. Use the *Services to Monitor* parameters to select the services that you want to monitor.
Event severity when a service is not found	Set the severity level, from 1 to 40, to indicate the importance of an event in which a monitored service cannot be found on the Contact Center server. The default is 25.
Monitor Service Availability	
Event Notification	
Raise event if a service is down?	Set to **Yes** to raise an event if a monitored service is unavailable. The default is Yes. Use the *Services to Monitor* parameters to select the services that you want to monitor.
Event severity when a service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which a monitored service is unavailable. The default is 25.
Data Collection	
Collect data for service availability?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the availability of specified services. The default is unchecked.
Services to Monitor	
Monitor ...	Set to **Yes** to monitor any combination of the listed services. By default, all services are monitored except Host Application Integration and TAO NT Naming Service.

SkillsetTimes

Use this Knowledge Script to monitor the amount of time that Contact Center skillsets spent in the following states:

- Active Time
- All Agents Busy Time
- Staffed Time

This script raises an event if the amount of time in any state exceeds the threshold that you set. In addition, this script generates data streams for the percentage of time and total number of minutes that a skillset spent in a particular state.

A *skillset* is a component of skill-based routing, which matches contacts to the most qualified Contact Center agent. The most qualified agent is the agent with the appropriate skillset or unique abilities for handling the type of call or contact.

Resource Object

NT_NORTELCC_APPSKILLSET

The TreeView pane of the Operator Console contains Application and Skillset objects under the NortelCC object. Within the Application and Skillset object folders are Application/Skillset (AppSkillset) pairs. The same pairs are represented within the Application and Skillset object folders. Their placement within the Application and Skillset folders allows you to search for a particular pair by either Application or Skillset. You can drop this Knowledge Script on a pair in either location.

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SkillsetTimes job fails. The default is 5.
Raise event if SQL query fails?	Set to **Yes** to raise an event if the SQL query fails. The default is Yes. AppManager uses a SQL query to retrieve Contact Center database configuration information.
Event severity when SQL query fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the SQL query fails to retrieve database configuration information. The default is 15.
Raise event if no new data found?	Set to **Yes** to raise an event if skillset data has not changed since the last time the script ran. The default is Yes.
Event severity when no new data found	Set the event severity level, from 1 to 40, to reflect the importance of an event in which skillset data has not changed since the last time the script ran. The default is 15.

Parameter	How to Set It
Monitor Total Active Time	
Data Collection	
Collect data for total Active time?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of minutes that skillsets spent in the Active state during the monitoring period. The default is unchecked.
Monitor Total All Agents Busy Time	
Data Collection	
Collect data for total All Agents Busy time?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of minutes that skillsets spent in the All Agents Busy state during the monitoring period. The default is unchecked.
Monitor Percentage of Time All Agents Busy	
Event Notification	
Raise event if percentage of time All Agents Busy exceeds threshold?	Set to **Yes** to raise an event if the percentage of time that skillsets spent in the All Agents Busy state exceeds the threshold that you set. The default is Yes.
Threshold - Maximum percentage of time All Agents Busy	Specify the maximum percentage of time that skillsets can spend in the All Agents Busy state before an event is raised. The default is 70%.
Event severity when percentage of time All Agents Busy exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of time that skillsets spent in the All Agents Busy state exceeds the threshold that you set. The default is 15.
Data Collection	
Collect data for percentage of time All Agents Busy?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of time that skillsets spent in the All Agents Busy state during the monitoring period. The default is unchecked.
Monitor Total Staffed Time	
Data Collection	
Collect data for total Staffed time?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of minutes that skillsets spent in the Staffed state during the monitoring period. The default is unchecked.

SystemUsage

Use this Knowledge Script to monitor Contact Center usage of system resources: CPU, interrupts, page faults, committed bytes, CLAN, and ELAN. This script raises an event if a value exceeds the threshold that you set.

This script generates data streams for the following metrics:

- CPU utilization: average and instantaneous (%)
- Interrupts per second (#)
- Committed bytes (%) as a percentage of the commit limit
- CLAN utilization (%). CLAN is the network used to communicate application information between the Contact Center server and customer applications.
- ELAN utilization (%). ELAN is the network used to communicate management information between the Contact Center server, the Call Pilot server, and the Nortel Communications Server switch.

Resource Object

NT_NortelCC_SCCS

Default Schedule

By default, this script runs every minute.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SystemUsage job fails. The default is 5.
Raise event if an error occurs reading a perfmon counter?	Set to **Yes** to raise an event if the script encounters a problem in reading the Performance Monitor counter for a particular metric. The default is Yes.
Event severity when an error occurs reading a perfmon counter	Set the severity level, from 1 to 40, to indicate the importance of an event in which the script encountered a problem in reading the Performance Monitor counter for a particular metric. The default is 40.
Raise event if a perfmon counter is invalid or unusable?	Set to **Yes** to raise an event if the Performance Monitor counter for a particular metric is invalid or unusable. The default is Yes.
Event severity when a perfmon counter is invalid or unusable	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Performance Monitor counter for a particular metric is invalid or unusable. The default is 40.
Raise event if a WMI error occurs	Set to **Yes** to raise an event if the script encounters a WMI (Windows Management Instrumentation) error. The default is Yes. This script uses WMI to retrieve performance metrics from the Windows operating system.

Parameter	How to Set It
Event severity when a WMI error occurs	Set the severity level, from 1 to 40, to indicate the importance of an event in which the script encounters a WMI error. The default is 40.
Monitor Instantaneous CPU Utilization	
Event Notification	
Raise event if instantaneous CPU utilization exceeds threshold?	Set to **Yes** to raise an event if the percentage of instantaneous CPU utilization exceeds the threshold that you set. The default is Yes. Instantaneous CPU utilization is the value at the moment the data was collected.
Threshold - Maximum instantaneous CPU utilization	Specify the maximum percentage of instantaneous CPU utilization that can occur before an event is raised. The default is 99%.
Event severity when instantaneous CPU utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of instantaneous CPU utilization exceeds the threshold. The default is 25.
Data Collection	
Collect data for instantaneous CPU utilization?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of instantaneous CPU utilization for the monitoring period. The default is unchecked.
Monitor Average CPU Utilization	
Event Notification	
Raise event if average CPU utilization exceeds threshold?	Set to **Yes** to raise an event if the percentage of average CPU utilization exceeds the threshold that you set. The default is Yes.
Threshold - Maximum average CPU utilization	Specify the maximum percentage of average CPU utilization that can occur before an event is raised. The default is 50%.
Event severity when average CPU utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of average CPU utilization exceeds the threshold. The default is 25.
Data Collection	
Collect data for average CPU utilization?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of average CPU utilization for the monitoring period. The default is unchecked.
Monitor Interrupts Per Second	
Event Notification	
Raise event if interrupts per second exceed threshold?	Set to **Yes** to raise an event if the number of interrupts that occur per second exceeds the threshold that you set. The default is Yes.
Threshold - Maximum interrupts per second	Specify the maximum number of interrupts that can occur per second before an event is raised. The default is 3000 interrupts.
Event severity when interrupts per second exceed threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of interrupts that occur per second exceeds the threshold. The default is 25.
Data Collection	
Collect data for interrupts per second?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of interrupts that occurred per second during the monitoring period. The default is unchecked.

Parameter	How to Set It
Monitor Committed Bytes as Percentage of Commit Limit	
Event Notification	
Raise event if committed bytes as percentage of commit limit exceeds threshold?	Set to **Yes** to raise an event if committed bytes (represented as a percentage of the commit limit) exceed the threshold that you set. The default is Yes. Committed bytes are those that have been allocated by processes. They are a measure of the demand for virtual memory. The commit limit is the amount of virtual memory, in bytes, that can be committed without having to extend the paging files.
Threshold - Maximum committed bytes as percentage of commit limit	Specify the maximum percentage of committed bytes that can occur before an event is raised. The default is 90%.
Event severity when committed bytes as percentage of commit limit exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of committed bytes exceeds the threshold. The default is 25.
Data Collection	
Collect data for committed bytes as percentage of commit limit?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of committed bytes for the monitoring period. The default is unchecked.
Monitor CLAN Utilization	
Event Notification	
Raise event if CLAN utilization exceeds threshold?	Set to **Yes** to raise an event if the percentage of CLAN utilization exceeds the threshold that you set. The default is Yes.
Threshold - Maximum CLAN utilization	Specify the maximum percentage of CLAN utilization that can occur before an event is raised. The default is 30%.
Event severity when CLAN utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of CLAN utilization exceeds the threshold. The default is 25.
Data Collection	
Collect data for CLAN utilization?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of CLAN utilization for the monitoring period. The default is unchecked.
Monitor ELAN Utilization	
Event Notification	
Raise event if ELAN utilization exceeds threshold?	Set to **Yes** to raise an event if the percentage of ELAN utilization exceeds the threshold that you set. The default is Yes.
Threshold - Maximum ELAN utilization	Specify the maximum percentage of ELAN utilization that can occur before an event is raised. The default is 30%.
Event severity when ELAN utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the percentage of ELAN utilization exceeds the threshold. The default is 25.
Data Collection	
Collect data for ELAN utilization?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the percentage of ELAN utilization for the monitoring period. The default is unchecked.

Chapter 51
NortelCS Knowledge Scripts

AppManager for Nortel Communication Server 1000 provides Knowledge Scripts that enable you to monitor Nortel CS1000 devices. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or, from within the Operator Console, select a Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
Alarms	Monitors the proxy agent computer for Nortel CS1000 alarms.
BMZ_CallQuality	Monitors call quality statistics for Bandwidth Management Zones (BMZs) for Nortel CS1000 versions 4.50 and later.
CallCapacity	Retrieves the call capacity utilization calculation from a Call Server for Nortel CS1000 versions 4.50 and 5.0.
GetOMReport	Retrieves the most recent Operational Management (OM) report and the report from the previous day, if one exists.
HealthCheck	Monitors the state of the Call Server, Media Gateway Controller, Signaling Server, MC32S, Network Routing Server, VGMC, and SIP Gateway.
PhoneInventory	Creates an inventory of IP phones based on data from the Call Server Entity MIB.
SS_CallQuality	Monitors Signaling Server statistics: jitter, latency, voice time, audio setups, and lost packets. This script also monitors R-factor for Nortel CS1000 versions 4.0 and later.
SS_H323Stats	Monitors Signaling Server H.323 trunk statistics: incoming voice and fax calls, and outgoing voice and fax calls.
SS_Registration	Monitors registration failures and attempts on the Signaling Server.
SS_SIPStats	Monitors Signaling Server SIP trunk statistics: incoming voice and fax calls, and outgoing voice and fax calls. **Note** This script supports Nortel CS1000 versions 4.0 and later.
VGMC_CallQuality	Monitors channel statistics of the VGMC, Media Gateway Controller, and MC32S: audio setups, voice time, average and maximum jitter, maximum average latency, and lost packets.

Alarms

Use this Knowledge Script to monitor Nortel CS1000 alarms. Call Servers, Signaling Servers, Media Gateways, MGCs, ECMs, NRSs, VGMCs and SIPL send alarms to the proxy agent computer using SNMP traps.

When setting parameters for this script, you will be asked to provide a list of alarm identifiers (system messages) to include or exclude from monitoring. System messages are discussed in the Nortel CS1000 *Software Input/Output System Message* publication (Nortel publication number 553-3001-411). Their format consists of a multi-letter code followed by a multi-digit alarm number, such as AUD000 or SRPT194.

Running this Knowledge Script job consumes approximately 20 MB of memory, per instance, on the proxy agent computer.

This script can launch an Action Knowledge Script that triggers NetIQ Vivinet Diagnostics to diagnose the problem when QoS alarms are raised. For more information, see the Help for the Action_DiagnoseNortelIPT Knowledge Script.

Prerequisites

- Install the Windows SNMP service. If you installed the service *before* you installed the AppManager for Nortel CS1000 module, then you do not need to do anything else. If you installed the service *after* you installed the module, then stop and restart the proxy agent computer before using this script.
- Configure Nortel CS1000 devices to send SNMP traps to the proxy agent computer. For more information, see "Identifying the SNMP Trap Receiver" on page 2992.
- The AppManager for Nortel CS1000 module is incompatible with the Nortel Telephony Manager application, which competes with the module for UDP port 162. AppManager will not receive SNMP traps if Telephony Manager is installed.
- The AppManager for Nortel CS1000 module is incompatible with NetIQ SNMP Trap Receiver (Trap Receiver), which competes with the module for UDP port 162. AppManager will not receive SNMP traps if Trap Receiver is installed.

Resource Objects

NortelCS Call Server

NortelCS Signaling Server

NortelCS VGMC

NortelCS Media Gateway Controller

NortelCS MC32S

NortelCS Network Routing Server

NortelCS Enterprise Common Manager

NortelCS SIP Line

Important

In most circumstances, the Alarms Knowledge Script raises events for alarms (traps) received from the Nortel CS1000 component on which you run the job. The component ID property of each trap identifies the source of the trap. For example, a component ID of "CS" identifies the Call Server. The component ID also determines which resource object an event is raised against.

For environments in which a co-resident server hosts multiple applications, the component ID may not correctly identify the source of a trap. When the component ID incorrectly identifies the source of a trap, events are raised against the incorrect resource object.

For example, if a co-resident server hosts the Call Server, the Signaling Server, and the Network Routing Server (NRS), the component ID may indicate a trap was received from the NRS. In addition, the event will be raised against the NRS object. However, experience may tell you that the trap actually came from the Signaling Server.

To ensure events are raised for all traps received from all components on a co-resident server, run the Alarms Knowledge Script on the co-resident server parent object so that all component child objects are monitored. If you run the Alarms job on only the Signaling Server, for example, AppManager will not raise an event for the Signaling Server trap that is incorrectly identified as an NRS trap.

Default Schedule

By default, this script runs on an asynchronous schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Notes for the "critical to monitor" and QoS alarm categories: • If you "Include" selected alarm identifiers in a category, AppManager raises events for those alarm identifiers plus the identifiers that are, by default, included in the category. • If you "Include only" selected alarm identifiers in a category, AppManager raises events *only* for those identifiers. *AppManager will not raise events for the other identifiers included in the category*. • If you "Exclude" selected alarm identifiers from a category, AppManager raises events for all alarm identifiers included in the category *except* those you specifically excluded. • If you accept the default settings in the *Alarm identifiers* parameters, "Exclude" and blank, AppManager raises events for all identifiers in the category, because you excluded nothing from the category.	
Monitor "critical to monitor" alarms?	Select **Yes** to monitor alarms in the "critical to monitor" category. The default is Yes.
Include or exclude alarms?	Select whether you want to **Include**, **Include only**, or **Exclude** the alarm identifiers you specify in the following parameter. • Select **Include** to *add* the listed identifiers to the "critical to monitor" category. • Select **Include only** to include *only* the listed identifiers in the "critical to monitor" category. • Select **Exclude** to exclude the listed identifiers from the "critical to monitor" category. This is the default option. By default, the "critical to monitor" category includes all alarms designated as "critical to monitor" in the Nortel CS1000 *Software Input/Output System Messages* publication (Nortel publication number 553-3001-411).
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the "critical to monitor" category. The default is an empty list.
Monitor QoS alarms?	Select **Yes** to monitor the proxy agent computer for alarms in the QoS category. The default is Yes.
Include or exclude alarms?	Select whether you want to **Include**, **Include only**, or **Exclude** the alarm identifiers you specify in the *Alarm identifiers* parameter. • Select **Include** to *add* the listed identifiers to the QoS category. • Select **Include only** to include *only* the listed identifiers in the QoS category. • Select **Exclude** to exclude the listed identifiers from the QoS category. This is the default option. By default, the QoS category includes the following alarms for Nortel CS1000 versions 4.0, 4.50, 5.0, and 6.0: ITG1028, ITG2028, ITG3028, ITG4028, ITG4043, ITG4044, QOS0012, QOS0013, QOS0014, QOS0015, QOS0017, QOS0018, QOS0019, QOS0020, QOS0022, QOS0024, QOS0026, QOS0028, QOS0030, QOS0032, QOS0034, QOS0036, QOS0038, QOS0039, QOS0040, QOS0041, QOS0042, QOS0043
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the "QoS" category. The default is an empty list.
Phone filter	

Parameter	How to Set It
Include or exclude phones?	You can use IP addresses to further filter the results of the QoS alarm monitoring. Select whether you want to **Include only** or **Exclude** the IP addresses you specify in *Phone IP addresses* or *Phone IP address ranges*. AppManager will monitor — or exclude — QoS alarms related to the calling and called phones that belong to the IP addresses. • Select **Include only** to monitor QoS alarms *only* the listed phone IP addresses. • Select **Exclude** to exclude listed phone IP addresses from QoS alarm monitoring. This is the default option
Phone IP addresses	Provide a comma-separated list of the IP addresses of the phones you want to monitor for QoS alarms. For example: `10.14.2.21,10.14.3.100,10.14.1.50`
Phone IP address ranges	Type a comma-separated list of IP address ranges for the phones you want to monitor for QoS alarms. For example: `10.14.2.21-10.14.3.100,10.14.1.10-10.14.1.50`
Launch Diagnostics when the following alarm is received ...	
Warning packet loss QOS0022?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0022 alarm is raised. The default is unselected.
Warning latency QOS0024?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0024 alarm is raised. The default is unselected.
Warning jitter QOS0026?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0026 alarm is raised. The default is unselected.
Warning R-factor QOS0028?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0028 alarm is raised. The default is Yes.
Unacceptable packet loss QOS0030?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0030 alarm is raised. The default is unselected.
Unacceptable latency QOS0032?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0032 alarm is raised. The default is unselected.
Unacceptable jitter QOS0034?	Select **Yes** to launch Vivinet Diagnostics to diagnose the problem when the QOS0034 alarm is raised. The default is unselected.
Note for the following alarm categories: AppManager raises an event **only** for those alarm identifiers you specifically include, or it raises an event for all alarm identifiers **except** those you specifically exclude. If you accept the default of an empty list in the *Alarm identifiers* parameters, AppManager raises events for **all** alarm identifiers.	
Monitor critical alarms?	Select **Yes** to monitor alarms in the critical category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. • Select **Include only** to include *only* the listed identifiers in the critical category. • Select **Exclude** to exclude the listed identifiers from the critical category. This is the default value. By default, the critical category includes all alarms with critical severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the critical category. The default is an empty list.
Monitor major alarms?	Select **Yes** to monitor alarms in the major category. The default is unselected.

Parameter	How to Set It
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. • Select **Include only** to include *only* the listed identifiers in the major category. • Select **Exclude** to exclude the listed identifiers from the major category. This is the default option. By default, the major category includes all alarms with major severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the major category. The default is an empty list.
Monitor minor alarms?	Select **Yes** to monitor alarms in the minor category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. • Select **Include only** to include *only* the listed identifiers in the minor category. • Select **Exclude** to exclude the listed identifiers from the minor category. This is the default option. By default, the minor category includes all alarms with minor severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the minor category. The default is an empty list.
Monitor warning alarms?	Select **Yes** to monitor alarms in the warning category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. • Select **Include only** to include *only* the listed identifiers in the warning category. • Select **Exclude** to exclude the listed identifiers from the warning category. This is the default option. By default, the warning category includes all alarms with warning severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the warning category. The default is an empty list.
Monitor info alarms?	Select **Yes** to monitor alarms in the informational category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. • Select **Include only** to include *only* the listed identifiers in the informational category. • Select **Exclude** to exclude the listed identifiers from the informational category. This is the default option. By default, the informational category includes all alarms with informational severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the informational category. The default is an empty list.
Monitor cleared alarms?	Select **Yes** to monitor alarms in the cleared category. The default is unselected.

Parameter	How to Set It
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. • Select **Include only** to include *only* the listed identifiers in the cleared category. • Select **Exclude** to exclude the listed identifiers from the cleared category. This is the default option. By default, the cleared category includes all alarms with cleared severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the cleared category. The default is an empty list.
Monitor indeterminate alarms?	Select **Yes** to monitor alarms in the indeterminate category. The default is unselected.
Include or exclude alarms?	Select whether you want to **Include only** or **Exclude** the alarm identifiers you specify in the following parameter. • Select **Include only** to include *only* the listed identifiers in the indeterminate category. • Select **Exclude** to exclude the listed identifiers from the indeterminate category. By default, the indeterminate category includes all alarms with indeterminate severity in the SNMP trap.
Alarm identifiers	Provide a comma-separated list of the alarm identifiers you want to include in or exclude from the indeterminate category. The default is an empty list.
Event Severities	
Severity - Critical alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a critical alarm is detected. The default is 10.
Severity - Major alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a major alarm is detected. The default is 15.
Severity - Minor alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a minor alarm is detected. The default is 20.
Severity - Warning alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a warning alarm is detected. The default is 25.
Severity - Info alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which an informational alarm is detected. The default is 30.
Severity - Cleared alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which a cleared alarm is detected. The default is 30.
Severity - Indeterminate alarms	Set the severity level, between 1 and 40, to indicate the importance of an event in which an indeterminate alarm is detected. The default is 30.

Understanding an Alarms Event Message

The message on the Message tab of an event raised by the Alarms script provides not only a brief description of the event, but also recommends any corrective action you can take. AppManager retrieves the recommended actions from a database provided by Nortel.

In the following example, the Alarms script raised an event for the ITS2008 alarm on a Signaling Server:

```
NTP index: ITS2008
Nortel CS device:SIG_SERV
Alarm: Terminal connection status: 10.40.101.112 lost
```

The Message tab for this event provided the following "Help" and "Recommended Action" for the alarm:

```
Help for ITS2008:
Terminal connection status: <terminalIP><ok/lost>.

Recommended action for ITS2008:
1. Alarm may indicate random occurrence that is not service impacting; note
occurrence time and date for further follow-up. If any service-impacting problems
occur at the same time, further analysis is required immediately. 2. If alarm
persists, log into device and capture maintenance report log (if possible) and
send the text to Nortel support staff via email. Follow any steps described above
for the specific alarm.
```

Occasionally, more than one Help is available for an alarm. In this case, all Helps are shown first:

```
NTP index: XMI0002
Extra diagnostic information: 18 MGATE

Help for XMI0002 XFIL 1:
Main fiber interface (MFI) local is operational.

Help for XMI0002 XFIR 2:
Expansion fiber interface (EFI) remote is operational in first expansion cabinet.

Help for XMI0002 XFIR 3:
Expansion fiber interface (EFI) remote is operational in second expansion
cabinet.

Help for XMI0002 I s c:
Card polling re-established.
```

Any Recommended Actions will follow the Helps. It is possible, though, for no Recommended Actions to be available.

The Event tab in an Alarms event message provides a one-line *Message* that briefly describes the problem detailed on the Message tab. For Nortel CS1000 version 5.x and 6.0 alarms, the message can look something like this example:

```
Critical alarm IOD0040: Raleigh CS1K:RTP:CS [10.42.1.11]
```

The format of this message is defined as follows:

```
<severity>alarm<index>: <navigation system name>:<navigation site
name>:<component> [<component IP address>]
```

The navigation system name and navigation site name are taken from the SNMP Configuration information you set in Element Manager.

Identifying the SNMP Trap Receiver

Configure Nortel CS1000 to send SNMP traps to the Nortel CS1000 proxy agent computer. The configuration procedures are different for Nortel CS1000 versions 4.0, 4.50, 5.x, and 6.0.

Configuring the Trap Receiver in Version 6.0

Use Unified Communications Manager or Element Manager to configure the trap receiver. To use Element Manager to configure the trap receiver, see "Configuring the Trap Receiver in Version 5.x" on page 2993.

To configure the trap receiver using Unified Communications Manager:

1. Navigate to **Network**, click **CS1000 Services**, and then click **SNMP Profiles**.
2. Click **SNMP Profile**.

3. Select the SNMP profile you want to use.

   Or, to create a new profile, click **Add** and specify a new name for an **Alarm** type of profile.

4. In the **Trap Destination IP address** field, provide the IP address of the proxy agent computer to which the Nortel devices should sent SNMP traps.

5. Click **Save**.

6. Click **SNMP Distribution**, and then select all Nortel devices that should send SNMP traps to the proxy agent computer.

7. Click **Assign**.

8. In the **Alarm Profile** field, select the SNMP profile name from Step 3.

Configuring the Trap Receiver in Version 5.x

Use Element Manager to configure the trap receiver.

To configure the trap receiver:

1. Navigate to **System**, click **Alarms**, and then click **SNMP**.

2. In the **Trap Destination IP address** field, provide the IP address of the proxy agent computer to which you want to send Call Server traps.

Configuring the Trap Receiver in Version 4.50

Use Element Manager to configure the trap receiver.

To configure the trap receiver:

1. Navigate to **System** and click **SNMP**.

   - In the **SNMP trap destination address** field, type the IP address of the proxy agent computer to which you want to send Call Server traps.

2. Navigate to **IP Telephony > Nodes > Configuration**.

   - Select the node ID for which you want to enable SNMP traps.
   - Click **Edit** and then select **SNMP** on the Edit page.
   - Click **Add** to create a new **IP address** field, and then enter the IP address of the proxy agent computer to which you want to send SNMP traps. Repeat for each IP address you want to add.
   - Select **Enable SNMP traps**.
   - Click **Save and Transfer**.

3. Repeat the items in Step 2 for each additional node ID you want to configure.

Configuring the Trap Receiver in Version 4.0

Use Element Manager to configure the trap receiver.

To configure the trap receiver:

1. Navigate to **Configuration**, click **IP Telephony**, and then click **SNMP Configuration**.
   - In the **SNMP trap destination address** field, type the IP address of the proxy agent computer to which you want to send Call Server traps.
2. Navigate to **Configuration**, click **IP Telephony**, and then click **Node Summary**.
   - Select the node ID for which you want to enable SNMP traps.
   - Click **Edit** and then click **SNMP**.
   - Click **Add** to create new **IP address** and **Subnet mask** fields, and then type the IP address and subnet mask of the proxy agent computer to which you want to send SNMP traps. Repeat for each IP address and subnet mask you want to add.
   - Select **Enable SNMP traps**.
   - Click **Save and Transfer**.
3. Repeat the items in Step 2 for each additional node ID you want to configure.

BMZ_CallQuality

Run this Knowledge Script to monitor blocked calls, peak bandwidth, and call quality metrics for Bandwidth Management Zones (BMZs) for intrazone and interzone traffic. AppManager retrieves call quality statistics from the Zone Traffic MIB on the Signaling Server. For Nortel CS1000 version 6.0, AppManager retrieves statistics from the Zone Traffic MIB on the Call Server.

You can use BMZs to prioritize or restrict the amount of bandwidth that can be consumed by voice traffic.

This script raises an event if zone statistics are unavailable, if the percentage of calls blocked and the percentage of peak bandwidth exceed the thresholds you set, and if call quality metrics exceed the thresholds you set in Element Manager more than *n* times in one hour. In addition, this script generates data streams for the call quality metrics you choose to monitor.

AppManager supports BMZ monitoring for Nortel CS1000 versions 4.50 and later.

Prerequisites

- For Signaling Server version 4.50, install Nortel patch `MPLR21714`. The patch requires configuration of the Call Server. Obtain the patch and its Readme from your Nortel support and maintenance provider.
- Configure BMZ QoS threshold levels in Nortel CS1000 Element Manager. For more information, see "Setting Bandwidth Management Zone Thresholds" on page 2999.
- For Nortel CS1000 versions 4.50 and 5.x, create user account **snmpqosq**. For more information, see "Enabling Access to the Signaling Server QoS MIB for Nortel CS1000 version 5.x" on page 2999.
- For Nortel CS1000 versions 4.50 and 5.x, ensure no user or application is logged into the Call Server when the Signaling Server attempts to retrieve zone statistics from the Call Server. The Signaling Server uses a special login to issue Overlay commands that allow it to retrieve zone statistics. The Signaling Server cannot retrieve statistics from a Call Server that is in use at the time of retrieval.

Understanding BMZ Call Data

The BMZ_CallQuality script monitors QoS and other IP statistics.

The Terminal Proxy Server in the Signaling Server extracts QoS statistics from the IP phones in an active call by periodically polling the phones during the length of the call. A Quality Detail Record (QDR) is created at the end of a call. A QDR is created for each segment of a call that is modified, perhaps by being transferred, conferenced, put on hold, or muted.

The QDR summarizes the overall **call quality** as good, warning, or unacceptable. Once created, the QDR is forwarded to the Call Server to be aggregated into interzone and intrazone statistics.

In addition to a summary of overall call quality, the QDR also contains QoS statistics that are collected for the duration of the call with respect to the incoming media stream: **latency, jitter, packet loss, and Listening R-factor**.

Peak bandwidth is the highest bandwidth reported in a call. Peak bandwidth and **average bandwidth** are expressed as percentages of the bandwidths configured for the zone.

The QDR contains QoS statistics *only* for Phase 2 phones.

The QDR categorizes each QoS statistic as good, warning, or unacceptable. The thresholds for these categories are user-configurable. The BMZ_CallQuality script raises events if a QoS statistic exceeds or falls below a threshold you set.

Resource Objects

Bandwidth Management Zone objects

For Nortel CS1000 versions 4.50 and 5.x, BMZ objects are children of the Signaling Server object. Run this script on only one Signaling Server per Call Server. All zones for your Nortel CS1000 deployment are displayed under every Signaling Server object. Limit your monitoring to one Signaling Server per Call Server to prevent this script from gathering duplicate data and generating duplicate data streams.

For Nortel CS1000 version 6.0, BMZ objects are children of the Call Server.

You can run this script on a top-level object, and then use the Objects tab to select the specific BMZ objects you want to monitor.

Default Schedule

By default, this script runs at ten minutes past the hour. Do not change this schedule. The Zone Traffic MIB is updated on the hour. By retrieving call quality metrics at ten minutes past the hour, you receive most recent data. Because the MIB is updated only once each hour, you do not need to run this script more than once an hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if zone statistics are inaccessible?	Select **Yes** to raise an event if BMZ statistics are inaccessible. The default is Yes. BMZ statistics are inaccessible if the Zone Traffic MIB from which they are retrieved does not respond to SNMP queries before the end of the interval specified in the *Timeout* parameter.
Timeout	Specify the length of time AppManager should attempt to access the Zone Traffic MIB before raising an event indicating zone statistics are inaccessible. The default is 300 seconds, which is equal to 300 attempts. **Note** For Nortel CS1000 versions 4.50 and 5.x, AppManager cannot access the MIB if a user or application is logged into the Call Server, and will retry the attempt once each second during the timeout interval.
Event severity when zone statistics are inaccessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which BMZ statistics cannot be retrieved. The default is 15.
Select traffic type	Select the type of call traffic you want to monitor: • **Interzone**: calls made between zones • **Intrazone**: calls made within a zone • **Interzone and intrazone**: calls made between and within zones. This is the default selection.
Interzone	
Event Notification	
Raise event if % of calls blocked exceeds threshold?	Select **Yes** to raise an event if the percentage of blocked interzone calls exceeds the threshold you set. The default is Yes. AppManager calculates the percentage of calls blocked as: $\frac{\text{callsBlocked}}{\text{callsMade} + \text{callsBlocked}}$

Parameter	How to Set It
Event severity when % of calls blocked exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of blocked interzone calls exceeds the threshold you set. The default is 15.
Raise event if peak bandwidth exceeds threshold?	Select **Yes** to raise an event if the percentage of interzone peak bandwidth exceeds the threshold you set. The default is Yes.
Event severity when peak bandwidth exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of interzone peak bandwidth exceeds the threshold you set. The default is 15.
Raise event if call quality exceeds threshold?	Select **Yes** to raise an event if interzone call quality exceeds one or more of the thresholds you set in the Call Quality parameters. The default is Yes.
Event severity when call quality exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which interzone call quality exceeds one or more of the thresholds you set in the Call Quality parameters. The default is 15.
Monitoring	
Threshold - Maximum % of calls blocked	Specify the highest percentage of calls that can be blocked in one hour in interzone traffic before an event is raised. The default is 15%.
Threshold - Maximum peak bandwidth	Specify the highest percentage of peak bandwidth utilization that can occur in one hour in interzone traffic before an event is raised. The default is 90%.
Call Quality	
Threshold - Maximum occurrences of listen R-factor warnings	Specify the maximum number of times in one hour the listen R-factor value can fall below the warning threshold in interzone traffic before an event is raised. The default is 0. You set the R-factor threshold in Element Manager.
Threshold - Maximum occurrences of unacceptable lost packets	Specify the maximum number of times in one hour the unacceptable lost packets threshold can be exceeded in interzone traffic before an event is raised. The default is 0. You set the lost packets threshold in Element Manager.
Threshold - Maximum occurrences of unacceptable jitter	Specify the maximum number of times in one hour the unacceptable jitter threshold can be exceeded in interzone traffic before an event is raised. The default is 0. You set the jitter threshold in Element Manager. Jitter is the mean deviation of the difference in RTP data packet spacing at the receiver compared to the sender for a pair of packets.
Threshold - Maximum occurrences of unacceptable latency	Specify the maximum number of times in one hour the unacceptable latency threshold can be exceeded in interzone traffic before an event is raised. The default is 0. You set the latency threshold in Element Manager. Latency is the average value of the difference between the time stamp indicated by the senders of messages and the timestamp of the receivers, measured when the messages are received. The average is obtained by adding all of the estimates, then dividing by the number of received messages.
Intrazone	
Event Notification	

Parameter	How to Set It
Raise event if % of calls blocked exceeds threshold?	Select **Yes** to raise an event if the percentage of intrazone calls blocked exceeds the threshold you set. The default is Yes. AppManager calculates the percentage of calls blocked as: $\frac{\text{callsBlocked}}{\text{callsMade} + \text{callsBlocked}}$
Event severity when % of calls blocked exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of intrazone calls blocked exceeds the threshold you set. The default is 15.
Raise event if peak bandwidth exceeds threshold?	Select **Yes** to raise an event if the percentage of intrazone peak bandwidth exceeds the threshold you set. The default is Yes.
Event severity when peak bandwidth exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which the percentage of intrazone peak bandwidth exceeds the threshold you set. The default is 15.
Raise event if call quality exceeds threshold?	Select **Yes** to raise an event if intrazone call quality exceeds one or more of the thresholds you set in the Call Quality parameters. The default is Yes.
Event severity when call quality exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which intrazone call quality exceeds one or more of the thresholds you set in the Call Quality parameters. The default is 15.
Monitoring	
Threshold - Maximum % of calls blocked	Specify the highest percentage of calls that can be blocked in one hour in intrazone traffic before an event is raised. The default is 15%.
Threshold - Maximum peak bandwidth	Specify the highest percentage of peak bandwidth utilization that can occur in one hour in intrazone traffic before an event is raised. The default is 90%.
Call Quality	
Threshold - Maximum occurrences of listen R-factor warnings	Specify the maximum number of times in one hour the listen R-factor value can fall below the warning threshold in intrazone traffic before an event is raised. The default is 0. You set the R-factor threshold in Element Manager.
Threshold - Maximum occurrences of unacceptable lost packets	Specify the maximum number of times in one hour the unacceptable lost packets threshold can be exceeded in intrazone traffic before an event is raised. The default is 0. You set the lost packets threshold in Element Manager.
Threshold - Maximum occurrences of unacceptable jitter	Specify the maximum number of times in one hour the unacceptable jitter threshold can be exceeded in intrazone traffic before an event is raised. The default is 0. You set the jitter threshold in Element Manager. Jitter is the mean deviation of the difference in RTP data packet spacing at the receiver compared to the sender for a pair of packets.

Parameter	How to Set It
Threshold - Maximum occurrences of unacceptable latency	Specify the maximum number of times in one hour the unacceptable latency threshold can be exceeded in intrazone traffic before an event is raised. The default is 0. You set the latency threshold in Element Manager. Latency is the average value of the difference between the time stamp indicated by the senders of messages and the timestamp of the receivers, measured when the messages are received. The average is obtained by adding all of the estimates, then dividing by the number of received messages.
Collect data?	Select **Yes** to collect data for reports and graphs. The default is unselected. This script generates the following data streams, depending on the type of traffic you choose to monitor: • Total number of sampling intervals • Total intrazone/interzone calls • Total intrazone/interzone calls blocked • Average bandwidth percentage of intrazone/interzone traffic • Peak bandwidth percentage of intrazone/interzone traffic • Number of instances of unacceptable latency in intrazone/interzone traffic • Number of instances of unacceptable packet loss in intrazone/interzone traffic • Number of instances of unacceptable jitter in intrazone/interzone traffic • Number of instances of listen R-factor warnings in intrazone/interzone traffic

Setting Bandwidth Management Zone Thresholds

Before gathering Bandwidth Management Zone (BMZ) call quality metrics with the BMZ_CallQuality script, configure QoS zone basis threshold levels in Nortel CS1000 Element Manager.

To configure BMZ QoS thresholds:

1. Navigate to **Configuration**, click **IP Telephony**, and then click **Quality Of Service Thresholds**.

   or

   In version 5.x, navigate to **System**, click **IP Network**, and then click **QoS Thresholds**.

2. Set the **Warning** and **Unacceptable** thresholds appropriate for your environment. Call quality metrics that fall outside of the thresholds more than *n* times in an hour will be identified by the BMZ_CallQuality script.

3. Click **Submit**.

4. Use Element Manager or Overlay 43 to perform a Call Server data dump.

Enabling Access to the Signaling Server QoS MIB for Nortel CS1000 version 5.x

Enable SNMP access to the QoS MIB (`QoS-MIB.mib`) on the Signaling Server. A dedicated Limited Access Password (LAPW) user account named `snmpqosq` provides this access. Create the user account in Overlay 117.

The QoS MIB is also known as the zone traffic report MIB.

For more information about creating the user account, see the "MIBs" chapter of the document titled *Communication Server 1000 Fault Management – SNMP* (document NN43001-719, version 01.03).

CallCapacity

Use this Knowledge Script to retrieve the calculated call capacity utilization (CCU) value from the Host Resource MIB on a Call Server. This script raises an event if CCU exceeds the threshold you set. In addition, this script generates a data stream for CCU.

Rated call capacity (RCC) is a function of idle time and the number of call attempts in an hour for a Call Server. It represents the maximum level at which a Call Server's CPU can operate and still maintain a high grade of service. RCC assumes the highest call traffic peak during a busy hour is 30% higher than the average traffic level. CCU is an indicator of the call traffic load on the Call Server and is calculated as follows:

$$CCU = 100 \times \frac{CallAttempts}{RCC}$$

The CallCapacity script retrieves the result of this calculation from the Host Resource MIB.

Prerequisites

- Nortel CS1000 Call Server, version 4.50 or 5.0. The CallCapacity script **does not support** other versions of the Call Server. Nortel removed the call capacity metric beginning with version 5.5 of the Call Server.
- AppManager for Network Device, build 6.2.24.0, at minimum

Resource Object

NortelCS Call Server

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if call capacity utilization exceeds threshold?	Select **Yes** to raise an event if call capacity utilization exceeds the threshold you set. The default is Yes.
Event severity when call capacity utilization exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event in which call capacity utilization exceeds the threshold. The default is 10.
Monitoring	

Parameter	How to Set It
Threshold - Maximum call capacity utilization	Specify the highest percentage of call capacity utilization that must be reached before an event is raised. The default is 80%.
Collect data?	Select **Yes** to collect data for charts, reports, and graphs. When enabled, data collection returns the percentage of call capacity utilization for the Call Server. The default is unselected. **Note** The CCU value is not available from the Call Server until 24 hours after a system restart. During that 24-hour window, only negative values are returned until the correct value is available. Therefore, the data stream for the CallCapacity script will be “0” until the correct CCU value has been calculated.

GetOMReport

Use this Knowledge Script to retrieve the latest Operational Measurement (OM) report from the Signaling Server, the VGMC, the MGC, and the MC32S. This script also retrieves the previous OM Report, if one is available.

Run GetOMReport on the Signaling Server resource object before running the following scripts:

- SS_CallQuality
- SS_H323Stats
- SS_Registration
- SS_SIPStats

Run GetOMReport on the VGMC, MGC, and MC32S resource objects before running the VGMC_CallQuality Knowledge Script.

Prerequisites

- The GetOMReport Knowledge Script automatically uses FTP to retrieve the OM Report from the Signaling Server, the VGMC, the MGC, and MC32S. Configure special FTP requirements in AppManager Security Manager. For more information, see "Configuring FTP Server Parameters" on page 3004.
- The script hangs in Running state unless you configured all required SNMP community strings, PDT passwords, and SL1 Level 1 logins and passwords, and ensured you cannot ping the TLAN interface of the Nortel CS1000 device.

Resource Objects

NortelCS Signaling Server

NortelCS VGMC

NortelCS Media Gateway Controller

NortelCS MC32S

Default Schedule

By default, this script runs once every hour, at five minutes past the hour. Do not change the default. Devices collect data for the OM Report at the top of each hour. You receive the most recent data if you retrieve the OM Report at five minutes past the hour.

By default, the call quality-related NortelCS Knowledge Scripts run once every hour, at ten minutes past the hour. Under most circumstances, you do not need to change the default schedule. Devices collect data for the Operational Measurement (OM) report at the top of each hour. The GetOMReport Knowledge Script retrieves the OM Report at five minutes past the hour. And you have to run GetOMReport before you can run the CallQuality scripts.

You probably run multiple instances of each script in order to collect the data you need. Running several virtually identical jobs at the same time could put a heavy strain on CPU usage.

If you want to run multiple instances of any NortelCS script, you should offset the schedules just a bit, one or two minutes, so you are not running all of the jobs at the same time.

Keep in mind the following:

- OM Reports are retrieved by the GetOMReport Knowledge Script
- OM Reports are collected hourly, at five minutes past the hour (by default)
- OM Reports are requested from Signaling Servers, VGMCs, MC32Ss, and MGCs by using SNMP, but are transferred by using FTP
- OM Reports generally grow to as large as 200K
- Multiple FTP sessions can interfere with SNMP requests for other OM Reports, thereby making the OM Reports unavailable

To alleviate FTP contention or to reduce bandwidth requirements, consider creating multiple GetOMReport jobs. Stagger the times by using the Schedule tab to change the **Starting at** time in the Frequency panel.

Note
Do not set the **Starting at** time for later than 12:58:00. You do not want to miss the creation of the OM Report, which happens on the hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if NortelCS_GetOMReport fails?	Select **Yes** to raise an event when this Knowledge Script fails to retrieve the latest OM Report. The default is Yes.
Event severity if NortelCS_GetOMReport fails	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the GetOMReport job fails. The default is 15.
FTP timeout	Specify the number of seconds to allow for the transfer of the OM Report before the job times out. The default is 60 seconds.

Configuring FTP Server Parameters

The AppManager for Nortel CS1000 module uses a built-in FTP (File Transfer Protocol) server to transfer Operational Measurement (OM) reports. If your FTP requirements do not fall within the category of "special" as defined below, you can use the built-in FTP server as-is. You do not need to complete the procedures in this topic.

If you have special FTP requirements, use the procedures in this topic to configure FTP parameters in AppManager Security Manager *before* you run the GetOMReport Knowledge Script.

If you do not have special FTP requirements, **do not** complete the following procedures. "Special" FTP requirements are defined as one or both of the following:

- You want to use IIS as the FTP server.
- Your proxy agent computer has two or more network interface cards (NICs).

Configuration for Using Two or More NICs

Whether you use the built-in FTP server or the IIS FTP server, configure AppManager Security Manager when your proxy agent computer has two or more NICs (network interface cards). Configure Security Manager in the following instances:

- You have a preference as to which NIC is used in the FTP process
- One NIC has access to the ELAN and the others do not

Notes

- If one NIC has access to the ELAN and another has access to the TLAN, ensure the binding order is such that the NIC connected to the ELAN is listed first.
- If you use NetIQ Vivinet Diagnostics to diagnose VoIP quality problems in your Nortel CS1000 environment, the proxy agent computer *must* also have TLAN connectivity.

On the Custom tab of Security Manager, complete the following fields:

Field	Description
Label	`NortelCS_FTP_IPAddress`
Sub-label	• *For a single Nortel CS1000 device*, type the IP address of the Signaling Server, VGMC, MC32S, or MGC. • *For all Nortel CS1000 devices*, type `default`. *All* devices will FTP OM Reports to the FTP server listening on the IP address you specify in the **Value 1** field.
Value 1	IP address of the FTP server that resides on the proxy agent computer. By identifying this IP address, you tell incoming connections which IP address to use when the computer has more than one NIC. This IP address should have access to the ELAN

Configuration for Using IIS as the FTP Server

To use IIS as the FTP server, configure the root directory, the login username, and the login password into AppManager Security Manager.

Configuring the Root Directory

Identify the IIS FTP root directory path in AppManager Security Manager. Ensure the FTP path is write enabled.

On the Custom tab of Security Manager, complete the following fields:

Field	Description
Label	`NortelCS_FTP_Path`
Sub-label	• *For a single Nortel CS1000 device*, type the IP address of the Signaling Server, VGMC, MC32S, or MGC. • *For all Nortel CS1000 devices*, type `default`. All devices will FTO the OM Reports to the FTP server directory path you specify in the **Value 1** and **Value 2** fields.
Value 1	Root directory of the FTP server. The FTP server root directory, called “local path” in IIS, must be write enabled.
Value 2	File directory path, relative to the root directory, of the folder where OM Report files are to be saved. If this value is not specified, the OM Report files are saved in the root directory path. **Note** Virtual directory paths for IIS FTP are not supported.

Configuring the Login Username and Password

In AppManager Security Manager, configure the login username and password required for accessing the IIS FTP server.

On the Custom tab of Security Manager, complete the following fields:

Field	Description
Label	`NortelCS_FTP_Login`
Sub-label	• *For a single Nortel CS1000 device*, type the IP address of the Signaling Server, VGMC, MC32S, or MGC. • *For all Nortel CS1000 devices*, type `default`.
Value 1	Login user name required for accessing the IIS FTP server. The user name should have access to the file directory, or root directory if the file directory is not specified.
Value 2	Login password associated with the user name you entered in the **Value 1** field
Extended application support	Encrypts the password in Security Manager. You must select this option.

HealthCheck

Use this Knowledge Script to monitor the state of the Call Server, Signaling Server, Media Gateway Controller (MGC), Voice Gateway Media Card (VGMC), MC32S (a 32-channel VGMC), Enterprise Common Manager (ECM), Network Routing Server (NRS), and SIP Gateway (SIPL). This script raises an event if a device is not responsive or is in an abnormal state. In addition, this script generates data streams for device availability or state.

Resource Objects

NortelCS Call Server

NortelCS Signaling Server

NortelCS VGMC

NortelCS Media Gateway Controller

NortelCS MC32S

NortelCS Network Routing Server

NortelCS Enterprise Common Manager

NortelCS SIPL

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if health check fails?	Select **Yes** to raise an event when the selected device is unresponsive or in an abnormal state. The default is Yes.
Event severity if health check failed	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the selected device is unresponsive or in an abnormal state. The default is 15.
Collect data?	Select **Yes** to collect availability data for reports and graphs. 100 indicates the device is available. 0 indicates the device is in any state that is not normal, or there is no response to SNMP. The default is unselected.

Understanding Event Messages

The following are two common error messages, accompanied by an explanation, a likely cause, and any operator action that may be needed.

<Device> unresponsive to SNMP:<IP address>

Explanation: The Call Server, MGC, Signaling Server, VGMC, MC32S, ECM, NRS, or SIPL is not responding to SNMP.

Likely cause: Normal message when item is unresponsive.

Operator action: Restart the device.

<Device> in abnormal state:IP address>

Explanation: The Call Server, MGC, Signaling Server, VGMC, MC32S, ECM, or NRS is not running in the proper state.

Likely cause: Normal message when state is abnormal.

Operator action: Change the state of the device.

PhoneInventory

Use this Knowledge Script to create an inventory of IP phones based on data in the Call Server Entity MIB. The inventory is in `.csv` format. This script raises an event if no IP phones are found.

Prerequisite

For CS1000 versions 4.0 and later, populate the Entity MIB with IP phone information. For more information, see "Configuring the Call Server to Count IP Phones" on page 3010.

Resource Object

NortelCS Call Server

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if NortelCS_PhoneInventory succeeds?	Select **Yes** to raise an event if the PhoneInventory job succeeds in creating an inventory. The default is Yes.
Event severity if NortelCS_PhoneInventory succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the PhoneInventory job succeeds in creating an inventory. The default is 30.
Raise event if NortelCS_PhoneInventory fails?	Select **Yes** to raise an event if the PhoneInventory job fails for any reason. The default is Yes.
Event severity if NortelCS_PhoneInventory fails	Set the severity level, between 1 and 40, to indicate the importance of an event in which the PhoneInventory job fails. The default is 15.
Raise event if no IP phones are found?	Select **Yes** to raise an event if no IP phones are found in the Entity MIB. The default is Yes.
Event severity if no IP phones are found	Set the severity level, between 1 and 40, to indicate the importance of an event in which the Entity MIB contains no IP phones. The default is 15.
Report directory's pathname	Specify the full local or UNC path to the root of the directory in which you want to save the phone inventory report, which will be titled `NortelCS_PhoneInventory_<IP address of Call Server>.csv`. Ensure the `NetIQmc` service (NetIQ AppManager Client Resource Monitor) is configured to run as a user that has access to the UNC path. The default setting of "local system" does not have access to the UNC path. Without access to the path, AppManager cannot save the inventory to the output folder. Leave this field blank to save the inventory report to the default location: `c:\Program Files\NetIQ\temp`

Configuring the Call Server to Count IP Phones

The PhoneInventory Knowledge Script job uses SNMP to query the Entity MIB on the Call Server and counts the number of IP telephones in the Entity MIB. However, for this process to work, you must issue two or three commands in Overlay 117:

- Tell the Call Server to generate the inventory report once every midnight
- Tell the Call Server to include the IP telephones from the inventory report in the Entity MIB
- Optional: Tell the Call Server to generate the inventory report immediately

Note
Do not issue the following commands if you are using Nortel CS1000 version 3.0. The following instructions apply only for versions 4.0 and later.

Issue the commands *before* running Discovery_NortelCS. If you run discovery before issuing the commands, AppManager raises an event indicating phone counting was unsuccessful because AppManager expects to find at least one phone.

Issue the following commands in Overlay 117:

```
INV MIDNIGHT SETS
INV ENTITY SETS ON
```

These two commands generate an inventory report at midnight and add the phones from the inventory report to the Entity MIB. Once the phones are added to the MIB, rerun Discovery_NortelCS.

If you do not want to wait until midnight to generate the inventory report and add the phones to the Entity MIB, issue a third Overlay 117 command:

```
INV GENERATE SETS
```

Note
The inventory report can take hours to complete, based on the number of phones, which is why it normally runs at midnight. Because the task that generates the inventory report on the CS1000 runs at a low priority, it should not interfere with call processing.

SS_CallQuality

Use this Knowledge Script to monitor call quality statistics on the Nortel Signaling Server: audio setups, voice time, average and maximum jitter, latency, lost packets, listening R-factor, and Mean Opinion Score (MOS). This script raises an event if a statistic exceeds the threshold you set. In addition, this script generates the following data streams:

- **Total number of audio setups**, which is the number of call legs established in a call. A simple call may have only one audio setup, but a conference call or a call on hold can have multiple audio setups.
- **Average and maximum percentage of lost data packets**, calculated based on the number of expected packets and the number of packets actually received. The number of packets received includes those that were late or duplicates. Packets that arrive late are not counted as lost. The presence of duplicate packets can result in a negative value for lost data.
- **Average and minimum listening MOS on the phones** (Nortel CS1000 versions 4.0 and later only). The Listening MOS value represents the overall quality of a call from the listener's perspective. The MOS is a number between 1 and 5. A MOS of 5 is excellent. A MOS of 1 is unacceptably bad. The MOS calculation considers measured items plus jitter buffer size. AppManager uses a modified version of the ITU (International Telecommunications Union) G.107 standard E-model equation to calculate the MOS. This algorithm is used to evaluate the quality of a transmission by factoring in the "mouth to ear" characteristics of a speech path.
- **Average and minimum listening R-factor on the phones** (Nortel CS1000 versions 4.0 and later only). The E-model equation that calculates MOS also calculates R-factor. R-factors range from 100 (excellent) to 0 (poor), and are a direct measure of call quality or transmission quality with respect to codec type and quality factors such as packet loss and delay. A Listening R-factor score represents call or transmission quality from a listener's perspective.
- **Total voice time**, in seconds, for all calls of a particular set type during the reporting period.
- **Average and maximum jitter for each selected phone model**. Jitter is the mean deviation of the difference in RTP data packet spacing at the receiver compared to the sender for a pair of packets.
- **Average and maximum latency for each selected phone model**. Latency is the average value of the difference between the time stamp indicated by the senders of messages and the timestamp of the receivers, measured when the messages are received. The average is obtained by adding all of the estimates, then dividing by the number of received messages.

For more information, see "Understanding How Data Streams are Calculated" on page 3013.

Tip for Using This Script

You can use the SS_CallQuality script to retrieve data about every Nortel CS1000 phone type in your environment. However, data streams are based on *all* selected phone types, not *each* selected phone type. So if you run SS_CallQuality and choose to monitor all phones types, you will not be able to tell which phone type is responsible for a high percentage of lost packets, for example.

To ensure the SS_CallQuality script provides values for individual phone types, run the script once for each phone type. For instance, run SS_CallQuality once to monitor the i2004 model phones. Then run it again to monitor i2050 model phones.

Note that phone model names changed with CS1000 versions 4.50, 5.0, and 6.0. The phone models you monitor on a 4.50 Signaling Server may not exist on a 5.0 Signaling Server.

Prerequisite

Run GetOMReport before running this script.

Resource Object

NortelCS Signaling Server

Default Schedule

By default, this script runs once every hour, at ten minutes past the hour. Do not change the default. Devices collect data for the OM Report on the hour. The GetOMReport Knowledge Script retrieves the OM Report at five minutes past the hour.

If you change the default schedule for this script, you risk not getting the latest data.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if audio setups exceed threshold?	Select **Yes** to raise an event if the number of audio setups exceeds the threshold you set. The default is unselected.
Event severity if audio setups exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of audio setups exceeds the threshold you set. The default is 15.
Raise event if voice time exceeds threshold?	Select **Yes** to raise an event if the duration of voice time exceeds the threshold you set. The default is unselected.
Event severity if voice time exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the amount of voice time exceeds the threshold you set. The default is 15.
Raise event if call quality threshold crossed?	Select **Yes** to raise an event if any of the call quality statistics exceeds or fails to meet the threshold you set. The default is Yes.
Event severity if call quality threshold crossed	Set the severity level, between 1 and 40, to indicate the importance of an event raised when any of the call quality statistics (MOS, R-factor, lost packets, maximum jitter, or maximum latency) exceeds or fails to meet) the threshold you set. The default is 15.
Monitoring	
Threshold - Maximum audio setups	Specify the highest number of audio setups that can occur before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum voice time	Specify the largest amount of voice time that can accrue before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Call Quality	
Score	Select whether you want to set a threshold for **R-factor** or **MOS**.
Threshold - Minimum listen R-factor	Specify the minimum R-factor score can that occur before an event is raised. The default is 70.
Threshold - Minimum listen MOS	Specify the minimum Mean Opinion Score (MOS) that can occur before an event is raised. The default is 3.6.

Parameter	How to Set It
Threshold - Maximum lost packets	Specify the highest percentage of packets that can be lost before an event is raised. The default is 1%.
Threshold - Maximum jitter	Specify the highest amount of jitter that can occur before an event is raised. The default is 60 milliseconds.
Threshold - Maximum latency	Specify the highest amount of latency that can occur before an event is raised. The default is 400 milliseconds.
Collect data?	Select **Yes** to collect data for reports and graphs. When enabled, data collection returns several data streams based on the thresholds you set. The default is unselected.
Phone model selection	Type a regular expression that defines which phone models you want to monitor. For example, type `2007` to monitor only the 2007 phone model. Type `.*2004` to monitor any phone model name that contains 2004, such as 3Pi2004, i2004, 2004, and 2004P2. Type `i200[124]` to monitor phone models i2001, i2002, and i2004. Leave this parameter blank to monitor all phone models. The default is blank.

Understanding How Data Streams are Calculated

AppManager retrieves Nortel CS1000 call metrics (audio setups, voice time, jitter, latency, R-factor, MOS, registration, and lost packets) from the Operational Measurement (OM) Reports created each hour on the Signaling Server, VGMC, MC32S, and MGC.

OM Reports provide call data per phone *model*, not per phone. For example, the OM Report identifies the average jitter for all of the i2004 model phones, but does not identify the jitter value for each phone of that model. In addition, the OM Report collects average and maximum values for jitter and latency, but only a single value for R-factor, voice time, registration, and audio setups.

Therefore, when you run a data collection script, it is important to understand that the resulting data streams are based on groups of phone types and are limited by the type of raw data available in the OM Report. The following table illustrates how each data stream is calculated:

Data Stream	What the OM Report Provides	How Data Stream is Calculated
Total number of audio setups	Total number of audio setups for each phone model	AppManager finds the total number of audio setups from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The total number of audio setups for type A is 3, for type B is 6, and for type C is 9. The total of these three values is 18, which is the value represented by the data stream.

Data Stream	What the OM Report Provides	How Data Stream is Calculated
Average jitter	Average amount of jitter for each phone model	AppManager computes a weighted average of all the phone models you choose to monitor, based on the OM Report values for total voice time and average jitter. For example, you choose to monitor three phone types. The average amount of jitter for type A is 1 ms, for type B is 2 ms, and for type C is 3 ms. The amount of voice time for the three phone types is 2, 3, and 4 seconds, respectively. AppManager computes the weighted average using the following formula, in which AJ = average jitter and VT = voice time: $\frac{(AJ_a \times VT_a) + (AJ_b \times VT_b) + (AJ_c \times VT_c)}{VT_a + VT_b + VT_c}$ In the formula, the products of average jitter and voice time for each phone type are added together and then divided by the sum of the voice time values. In this example, the computed weighted average jitter is 2.222.
Maximum jitter	Maximum amount of jitter for each phone model	AppManager finds the highest amount of maximum jitter from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The maximum amount of jitter for type A is 1 ms, for type B is 2 ms, and for type C is 3 ms. The maximum of these three values is 3 ms, which is the value represented by the data stream.
Average latency	Average amount of latency for each phone model	AppManager computes a weighted average of all the phone models you choose to monitor, based on the OM Report values for total voice time and average latency. For example, you choose to monitor three phone types. The average amount of latency for type A is 1 ms, for type B is 2 ms, and for type C is 3 ms. The amount of voice time for the three phone types is 2, 3, and 4 seconds, respectively. AppManager computes the weighted average using the following formula, in which AL = average latency and VT = voice time: $\frac{(AL_a \times VT_a) + (AL_b \times VT_b) + (AL_c \times VT_c)}{VT_a + VT_b + VT_c}$ In the equation, the products of average latency and voice time for each phone type are added together and then divided by the sum of the voice time values. In this example, the computed weighted average latency is 2.222.
Maximum latency	Maximum amount of latency for each phone model	AppManager finds the highest amount of maximum latency from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The maximum amount of latency for type A is 1 ms, for type B is 2 ms, and for type C is 3 ms. The maximum of these three values is 3 ms, which is the value represented by the data stream.

Data Stream	What the OM Report Provides	How Data Stream is Calculated
Average percentage of lost packets	Total percentage of lost packets for each phone model	AppManager computes a weighted average of all the phone models you choose to monitor, based on the OM Report values for total voice time and lost packets. For example, you choose to monitor three phone types. The percentage of lost packets for type A is 1%, for type B is 2%, and for type C is 3%. The amount of voice time for the three phone types is 2, 3, and 4 seconds, respectively. AppManager computes the weighted average using the following formula, in which LP = lost packets and VT = voice time: $\frac{(LP_a \times VT_a) + (LP_b \times VT_b) + (LP_c \times VT_c)}{VT_a + VT_b + VT_c}$ In the equation, the products of lost packets and voice time for each phone type are added together and then divided by the sum of the voice time values. In this example, the computed weighted average percentage of lost packets is 2.222.
Maximum percentage of lost packets	Maximum percentage of lost packets for each phone model	AppManager finds the highest percentage of lost packets from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The total percentage of lost packets for type A is 3, for type B is 6, and for type C is 9. The highest of these three values is 9, which is the value represented by the data stream.
Average listen MOS	N/A	AppManager converts the average R-factor value into MOS using a conversion formula provided by the ITU (International Telecommunications Union).
Minimum listen MOS	N/A	AppManager converts the minimum R-factor value into MOS using a conversion formula provided by the ITU (International Telecommunications Union).
Average listen R-factor	An R-factor value for each phone model	AppManager computes a weighted average of all the phone models you choose to monitor, based on the OM Report values for total voice time and R-factor. For example, you choose to monitor three phone types. The R-factor value for type A is 99, for type B is 97 and for type C is 95. The amount of voice time for the three phone types is 2, 3, and 4 seconds, respectively. AppManager computes the weighted average using the following formula, in which RF = R-factor and VT = voice time: $\frac{(RF_a \times VT_a) + (RF_b \times VT_b) + (RF_c \times VT_c)}{VT_a + VT_b + VT_c}$ In the equation, the products of R-factor and voice time for each phone type are added together and then divided by the sum of the voice time values. In this example, the computed weighted average listen R-factor is 96.56.
Minimum listen R-factor	An R-factor value for each phone model	AppManager finds the lowest R-factor value from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The R-factor value for type A is 99, for type B is 97 and for type C is 95. The lowest of these three values is 95, which is the value represented by the data stream.

Data Stream	What the OM Report Provides	How Data Stream is Calculated
Total registration attempts	A registration value for each phone model	AppManager finds the total number of registration attempts from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The total number of registration attempts for type A is 3, for type B is 6, and for type C is 9. The total of these three values is 18, which is the value represented by the data stream.
Total registration failures	A registration value for each phone model	AppManager finds the total number of registration failures from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The total number of registration failures for type A is 3, for type B is 6, and for type C is 9. The total of these three values is 18, which is the value represented by the data stream.
Total unregistration attempts	An unregistration value for each phone model	AppManager finds the total number of unregistration attempts from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The total number of unregistration attempts for type A is 3, for type B is 6, and for type C is 9. The total of these three values is 18, which is the value represented by the data stream.
Total voice time	Total amount of voice time for each phone model. This value includes the voice time for both phase 1 and phase 2 phones.	AppManager finds the total amount of voice time from all of the phone models you choose to monitor. For example, you choose to monitor three phone types. The total amount of voice time for type A is 20 seconds, for type B is 25, and for type C is 30. The total amount of these three values is 75, which is the value represented by the data stream.

SS_H323Stats

Use this Knowledge Script to monitor H.323 virtual trunk statistics for the Nortel Signaling Server: incoming voice and fax calls, and outgoing voice and fax calls. This script raises an event if a statistic exceeds the threshold you set. In addition, this script generates the following data streams:

- **Maximum amount of voice time** on the H.323 virtual trunk for all calls of a particular set type during the reporting period.
- **Number of incoming attempted and completed voice calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete incoming voice calls.
- **Number of outgoing attempted and completed voice calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete outgoing voice calls.
- **Number of incoming attempted and completed FAX calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete incoming FAX calls.
- **Number of outgoing attempted and completed FAX calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete outgoing FAX calls.

For more information, see "Understanding How Data Streams are Calculated" on page 3013.

Prerequisite

Run GetOMReport before running this script.

Resource Object

NortelCS Signaling Server

Default Schedule

By default, this script runs once every hour, at ten minutes past the hour. Do not change the default. Devices collect data for the OM Report on the hour. The GetOMReport Knowledge Script retrieves the OM Report at five minutes past the hour.

If you change the default schedule for this script, you risk not receiving the latest data.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if voice time exceeds threshold?	Select **Yes** to raise an event if the duration of voice time exceeds the threshold you set. The default is unselected.
Event severity if voice time exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the amount of voice time is greater than the threshold you set. The default is 15.

Parameter	How to Set It
Raise event if incomplete incoming voice calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete incoming voice calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete incoming voice calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete incoming voice calls exceeds the threshold you set. The default is 15.
Raise event if incomplete outgoing voice calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete outgoing voice calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete outgoing voice calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete outgoing voice calls exceeds the threshold you set. The default is 15.
Raise event if incomplete incoming fax calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete incoming fax calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete incoming fax calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete incoming fax calls exceeds the threshold you set. The default is 15.
Raise event if incomplete outgoing fax calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete outgoing fax calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete outgoing fax calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete outgoing fax calls exceeds the threshold you set. The default is 15.
Monitoring	
Threshold - Maximum voice time	Specify the largest amount of voice time that can accrue before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum incomplete incoming voice calls	Specify the largest number of incomplete incoming voice calls that can occur before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum incomplete outgoing voice calls	Specify the largest number of incomplete outgoing voice calls that can occur before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum incomplete incoming fax calls	Specify the largest number of incomplete incoming fax calls that can occur before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum incomplete outgoing fax calls	Specify the largest number of incomplete outgoing fax calls that can occur before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Collect data?	Select **Yes** to collect data for reports and graphs. When enabled, data collection returns data streams based on the thresholds you set. The default is unselected.

SS_Registration

Use this Knowledge Script to monitor registration attempts and failures on the Nortel Signaling Server. This script raises an event if the number of registration failures or attempts exceeds the threshold you set. In addition, this script generates the following data streams:

- Total number of registration attempts
- Total number of registration failures
- Total number of unregistration attempts

For more information, see "Understanding How Data Streams are Calculated" on page 3013.

Tip for Using This Script

You can to use the SS_Registration script to retrieve data about every Nortel CS1000 phone type in your environment. However, data streams are based on *all* selected phone types, not *each* selected phone type. So if you run SS_Registration and choose to monitor all phones types, you will not be able to tell which phone type is responsible for a high number of registration failures, for example.

The only way you can ensure the SS_Registration script provides values for individual phone types is to run the script once for each phone type. For instance, run SS_Registration once to monitor the i2004 model phones. Then run it again to monitor i2050 model phones.

Note that phone model names changed with CS1000 version 4.50, 5.0, and 6.0. The phone models you monitor on a 4.50 Signaling Server may not exist on a 5.0 Signaling Server.

Prerequisite

Run GetOMReport before running this script.

Resource Object

NortelCS Signaling Server

Default Schedule

By default, this script runs once every hour, at ten minutes past the hour. Do not change the default. Devices collect data for the OM Report on the hour. The GetOMReport Knowledge Script retrieves the OM Report at five minutes past the hour.

If you change the default schedule for this script, you risk not getting the latest data.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if registration attempts exceed threshold?	Select **Yes** to raise an event if the number of registration attempts exceeds the threshold you set. The default is unselected.

Parameter	How to Set It
Event severity if registration attempts exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of registration attempts exceeds the threshold you set. The default is 15.
Raise event if registration failures exceed threshold?	Select **Yes** to raise an event if the number of registration failures exceeds the threshold you set. The default is Yes.
Event severity if registration failures exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of registration failures exceeds the threshold you set. The default is 15.
Raise event if unregistration attempts exceed maximum?	Select **Yes** to raise an event if the number of unregistration attempts exceeds the threshold you set. The default is unselected.
Event severity if unregistration attempts exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of unregistration attempts exceeds the threshold you set. The default is 15.
Monitoring	
Threshold - Maximum registration attempts	Specify the largest number of registration attempts that can occur before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum registration failures	Specify the largest number of registration failures that can occur before an event is raised. The default is 0.
Threshold - Maximum unregistration attempts	Specify the largest number of unregistration attempts that can occur before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Collect data?	Select **Yes** to collect data for reports and graphs. When enabled, data collection returns data streams based on the thresholds you set. The default is unselected.
Phone model selection	Type a regular expression that defines which phone models you want to monitor. For example: • Type `2007` to monitor only the 2007 phone model. • Type `.*2004` to monitor any phone model name that contains 2004, such as 3Pi2004, i2004, 2004, and 2004P2. • Type `i200[124]` to monitor phone models i2001, i2002, and i2004. Leave this parameter blank to monitor all phone models. The default is blank.

SS_SIPStats

Use this Knowledge Script to monitor SIP virtual trunk statistics for the Nortel Signaling Server: incoming voice and fax calls, and outgoing voice and fax calls. This script raises an event if a statistic exceeds the threshold you set.

- **Maximum amount of voice time** on the SIP virtual trunk for all calls of a particular set type during the reporting period.
- **Number of incoming attempted and completed voice calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete incoming voice calls.
- **Number of outgoing attempted and completed outgoing voice calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete outgoing voice calls.
- **Number of incoming attempted and completed FAX calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete incoming FAX calls.
- **Number of outgoing attempted and completed FAX calls** for the H.323 or SIP virtual trunk. The number of completed calls is subtracted from the number of attempted calls to calculate the number of incomplete outgoing FAX calls.

For more information, see "Understanding How Data Streams are Calculated" on page 3013.

This script supports Nortel CS1000 version 4.0 and later.

Prerequisite

Run GetOMReport before running this script.

Resource Object

NortelCS Signaling Server

Default Schedule

By default, this script runs once every hour, at ten minutes past the hour. Do not change the default. Devices collect data for the OM Report on the hour. The GetOMReport Knowledge Script retrieves the OM Report at five minutes past the hour.

If you change the default schedule for this script, you risk not getting the latest data.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if voice time exceeds threshold?	Select **Yes** to raise an event if the duration of voice time exceeds the threshold you set. The default is unselected.

Parameter	How to Set It
Event severity if voice time exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the amount of voice time exceeds the threshold you set. The default is 15.
Raise event if incomplete incoming voice calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete incoming voice calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete incoming voice calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete incoming voice calls exceeds the threshold you set. The default is 15.
Raise event if incomplete outgoing voice calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete outgoing voice calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete outgoing voice calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete outgoing voice calls exceeds the threshold you set. The default is 15.
Raise event if incomplete incoming fax calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete incoming fax calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete incoming fax calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete incoming fax calls exceeds the threshold you set. The default is 15.
Raise event if incomplete outgoing fax calls exceed threshold?	Select **Yes** to raise an event if the number of incomplete outgoing fax calls exceeds the threshold you set. The default is Yes.
Event severity if incomplete outgoing fax calls exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of incomplete outgoing fax calls exceeds the threshold you set. The default is 15.
Monitoring	
Threshold - Maximum voice time	Specify the largest amount of voice time that can accrue before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum incomplete incoming voice calls	Specify the largest number of incomplete incoming voice calls that can occur before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum incomplete outgoing voice calls	Specify the largest number of incomplete outgoing voice calls that can occur before an event is raised. The default is 0.
Threshold - Maximum incomplete incoming fax calls	Specify the largest number of incomplete incoming fax calls that can occur before an event is raised. The default is 0.
Threshold - Maximum incomplete outgoing fax calls	Specify the largest number of incomplete outgoing fax calls that can occur before an event is raised. The default is 0.
Collect data?	Select **Yes** to collect data for reports and graphs. When enabled, data collection returns data streams based on the thresholds you set. The default is unselected.

VGMC_CallQuality

Use this Knowledge Script to monitor channel statistics for the Nortel Voice Gateway Media Card (VGMC), Media Gateway Controller (MGC), and MC32S: audio setup, voice time, jitter, lost packets, and channel latency. This script raises an event if a statistic exceeds the threshold you set. In addition, this script generates the following data streams:

- **Total number of audio setups**, which is the number of call legs established in a call. A simple call may have only one audio setup, but a conference call or a call on hold can have multiple audio setups.
- **Total amount of voice time** for all calls of a particular set type during the reporting period.
- **Average and maximum jitter**. Jitter is the mean deviation of the difference in RTP data packet spacing at the receiver compared to the sender for a pair of packets.
- **Average percentage of lost packets**, calculated based on the number of expected packets and the number of packets actually received. The number of packets received includes those that were late or duplicates. Packets that arrive late are not counted as lost. The presence of duplicate packets could result in a negative lost data amount.
- **Average channel latency** (not available from VGMCs). Latency is the average value of the difference between the time stamp indicated by the senders of messages and the timestamp of the receivers, measured when the messages are received. The average is obtained by adding all of the estimates, then dividing by the number of received messages.

For more information, see "Understanding How Data Streams are Calculated" on page 3013.

Prerequisite

Run GetOMReport before running this script.

Resource Objects

NortelCS VGMC

NortelCS Media Gateway Controller

NortelCS MC32S

Default Schedule

By default, this script runs once every hour, at ten minutes past the hour. Do not change the default. Devices collect data for the OM Report on the hour. The GetOMReport Knowledge Script retrieves the OM Report at five minutes past the hour.

If you change the default schedule for this script, you risk not retrieving the latest data.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if audio setups exceed threshold?	Select **Yes** to raise an event if the number of audio setups exceeds the threshold you set. The default is unselected.

Parameter	How to Set It
Event severity if audio setups exceed threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the number of audio setups exceeds the threshold you set. The default is 15.
Raise event if voice time exceeds threshold?	Select **Yes** to raise an event if the duration of voice time exceeds the threshold you set. The default is unselected.
Event severity if voice time exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the amount of voice time exceeds the threshold you set. The default is 15.
Raise event if call quality exceeds threshold?	Select **Yes** to raise an event if any of the call quality statistics exceeds the threshold you set. The default is Yes.
Event severity if call quality exceeds threshold	Set the severity level, between 1 and 40, to indicate the importance of an event raised when the call quality statistics (maximum lost packets or maximum jitter) exceed the threshold you set. The default is 15.
Monitoring	
Threshold - Maximum audio setups	Specify the highest number of audio setups that can occur before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Threshold - Maximum voice time	Specify the largest amount of voice time that can accrue before an event is raised. The default is 0. **Note** The default value has no significance and is not a recommended threshold value.
Call Quality	
Threshold - Maximum lost packets	Specify the highest average percentage of packets that can be lost before an event is raised. The default is 1%.
Threshold - Maximum jitter	Specify the highest amount of jitter that can occur before an event is raised. The default is 60 milliseconds.
Threshold - Maximum average latency	Specify the highest amount of average channel latency that can occur before an event is raised. The default is 60 milliseconds.
Collect data?	Select **Yes** to collect data for reports and graphs. When enabled, data collection returns data streams based on the thresholds you set. The default is unselected.

Chapter 52
NortelCS2x Knowledge Scripts

AppManager for Nortel CS2x provides Knowledge Scripts for monitoring Nortel Communication Server 2000 and 2100 resources.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AddPhone	Adds Nortel IP phones to the AppManager console for monitoring by the PhoneQuality and PhoneDiagnostic Knowledge Scripts.
CallActivity	Monitors completed and peak active calls.
CallAlert	Monitors for mid-call alerts raised when voice quality thresholds are exceeded. Can launch Vivinet Diagnostics to diagnose the problem if alerts are received.
CallFailures	Monitors the following line maintenance logs for call failure data: 101, 102, 104, 105, 115, 138, and 160. You can monitor all or some of these logs.
CallQuality	Monitors end-of-call voice quality statistics: jitter, latency, packet loss, MOS (Mean Opinion Score), and R-Value.
CollectorHealth	Starts the collector services and monitors their activity and availability.
LogQuery	Monitors the number of logs in user-specified reports.
OMQuery	Monitors the contents of specified fields in OM Reports.
PhoneDiagnostic	Launches Vivinet Diagnostics on-demand to diagnose call quality between two specified phones.
PhoneInventory	Creates an inventory of the phones configured for an Element Manager.
PhoneQuality	Monitors mid-call voice quality statistics: jitter, latency, packet loss, MOS (Mean Opinion Score), and R-Value.
RemovePhone	Removes a Nortel IP phone from the AppManager console.
RetrieveConfigData	Retrieves station configuration information from individual CICM Element Managers and stores it in the Nortel CS2x supplemental database for monitoring by the PhoneInventory script.
SetupSupplementalDB	Creates a Nortel CS2x supplemental database in which to store log files, OM Reports, call details, QoS information, and station configuration information.
Recommended Knowledge Script Group	Performs essential monitoring of your Nortel CS2x environment.

AddPhone

Use this Knowledge Script to add Nortel IP phones (stations) to the AppManager console. This script raises an event if specified phones are added successfully or cannot be added.

You must add a phone before you can monitor it with the PhoneQuality or PhoneDiagnostic Knowledge Script.

Use the RemovePhone Knowledge Script to remove a phone.

Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run RetrieveConfigData to populate the supplemental database. The IP addresses and Directory Numbers (DNs) of the phones you want to add must have an entry in the supplemental database, or the AddPhone job will fail.

Resource Object

NortelCS2x Station Folder

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the AddPhone job fails. The default is 5.
Configuration Settings	
Directory Numbers of phones to add	Provide the DNs of the phones you want to add. You can provide one DN or a list of DNs. If you enter a list, separate the entries with a comma. For example: `74567,74569,74571`. **Note** If you have more DNs than is convenient to enter in this field, you can list the DNs in a separate file and then use the following parameter to access that file.

Description	How To Set It

Full path to file with list of Directory Numbers of phones to add	Provide the full path to a file that contains a list of the Directory Numbers you want to add. Each address in the file should be on a separate line. For example:
	`74567`
	`74569`
	`74571`
	Because the file must be accessible from the agent computer, the path must be a local directory on the agent computer or a UNC path.
	Important If you provide a UNC path, then the `netiqmc` service must have access to the path.

Allow non-existent phones to be added?	Select **Yes** to add non-existent phones. A phone is non-existent if its number is not in the station table. You can add a non-existent phone if you are sure the phone is valid. For example, you may have just plugged in the phone and do not want to wait for a station table update to test it. The default is unselected.
Default Configuration Settings for Non-Existent Phones	
Default node ID	Provide the alpha-numeric CICM node identifier for the phone you want to add, such as `cicm-005`.
Default terminal ID	Provide the terminal identifier of the phone you want to add, which is usually a MAC address. For example, `31-38-00-0A-E4-01-DA-82`.
Event Notification	
Raise event if all phones are added successfully?	Select **Yes** to raise an event if each phone is successfully added to the AppManager console. The default is Yes.
Event severity when all phones are added successfully	Set the event severity level, from 1 to 40, to reflect the importance of an event in which each phone is added successfully. The default is 25.
Raise event if too many phones to add?	Select **Yes** to raise an event if, by running this job, you will have added more than 500 phones per office configured in the AppManager console. The default is Yes.
Event severity when too many phones to add	Set the event severity level, from 1 to 40, to reflect the importance of an event in which you have attempted to add more than 500 phones to an office configured in the AppManager console. The default is 15.

CallActivity

Use this Knowledge Script to monitor call activity on a selected CS2x. This script raises an event if the number of completed calls and the maximum number of concurrent active calls exceed the thresholds you set. In addition, this script generates data streams for completed and active calls.

This script uses the data collected by the OM file collector service and stored in the supplemental database.

Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run CollectorHealth to start the OM file collector service.

Resource Object

NortelCS2x

Default Schedule

By default, this script runs every five minutes.

You may notice a large difference between the timestamp of the data point (generated every five minutes on the default schedule) and the timestamp of the OM Report that provides the data for this script. The OM Report interval varies, but is typically every five, 30, or 60 minutes. The timestamp of the OM Report represents the beginning of the interval. For example, if the OM Report for the calls made from 9:00 to 9:30 is sent at 9:30, the timestamp is 9:00. The data point will have a timestamp of a few minutes past 9:30, depending on when the five-minute default interval ends.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallActivity job fails. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the OM file collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OM file collector service reports an error. The default is 5.
Raise event if data collector reports a transaction error?	Select **Yes** to raise an event if the OM file collector service reports a transaction error. The default is Yes.
Event severity when data collector reports a transaction error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OM file collector service reports a transaction error. The default is 10.

Parameter	How to Set It
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the OM file collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OM file collector service reports a warning. The default is 15.
Troubleshooting	
Select time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **Note** This parameter is valid only when you select **Run once** on the Schedule tab.
Location Filter	
Include or exclude specific locations	Select the IEMS systems for which you want to monitor call activity. • Select **Include only** to monitor call activity from the system specified in the *Location* parameter. • Select **Exclude** to monitor call activity for all systems except the system specified in the *Location* parameter. The default is Exclude.
Location	Provide the name of the IEMS system that you want to include or exclude from monitoring.
Monitor Total Completed Calls	
Event Notification	
Raise event if total number of completed calls exceeds threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum total number of completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 100 active call.
Event severity when total number of completed calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for total number of completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period. The default is Yes.
Monitor Concurrent Active Calls	
Event Notification	
Raise event if maximum number of concurrent active calls exceeds threshold?	Select **Yes** to raise an event if the maximum number of concurrent active calls exceeds the threshold you set. The default is Yes. *Concurrent active calls* are calls that are in progress at the same time during a monitoring interval. Use this set of parameters to monitor the maximum number of concurrent calls that are in progress at any point in time. For example, during a five-minute interval, ten calls are active at one moment, seven calls are active at another, and three active at yet another moment. Therefore, for this interval, the maximum number of concurrent active calls is ten.
Threshold - Maximum number of concurrent active calls	Specify the maximum number of concurrent calls that can be active at any point in time before an event is raised. The default is 100 active calls.

Parameter	How to Set It
Event severity when number of concurrent active calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of concurrent active calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for maximum number of concurrent active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the maximum number of concurrent calls that were active during the monitoring period. The default is Yes.

CallAlert

Use this Knowledge Script to monitor mid-call alerts (vqalerts) generated when voice quality metrics exceed or fall below a threshold you set on the CICM Element Manager. This script raises an event if vqalerts are generated. You can filter results by vqalert and by phone, and you can launch NetIQ Vivinet Diagnostics to diagnose the problem if vqalerts are generated. For more information, see "Triggering Call and Phone Quality Diagnoses" on page 3067.

Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run CollectorHealth to start the QoS syslog collector service.

Resource Object

NortelCS2x

Default Schedule

By default, this script runs on an asynchronous schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallAlert job fails. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the QoS syslog collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QoS syslog collector service reports an error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the QoS syslog collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QoS syslog collector service reports a warning. The default is 15.
Monitor Settings	
Perform traceroute and launch Vivinet Diagnostics when voice quality alert is received?	Select **Yes** to send a traceroute request to the CICM Element Manager and to launch Vivinet Diagnostics to diagnose the problem if vqalerts are received. The default is Yes.
Length of time to wait for traceroute responses	Specify the maximum length of time that the CallAlert job should wait for a response to traceroute requests to the CICM Element Manager. The CallAlert job will fail if the response time is longer than you specify. The default is 120 seconds.

Parameter	How to Set It
Raise event if voice quality alert is received?	Select **Yes** to raise an event if vqalerts are generated when voice quality metrics exceed the threshold you set on the CICM Element Manager. The default is Yes.
Event severity when voice quality alert is received	Set the severity level, from 1 to 40, to indicate the importance of an event in which vqalerts are generated when voice quality metrics exceed the threshold you set on the CICM Element Manager. The default is 15.
Include or exclude specific voice quality alerts	Indicate how to monitor the vqalerts you select in the *Alert filter* parameters. The default is Exclude. • Select **Include** to monitor only the selected vqalerts. • Select **Exclude** to monitor all vqalerts *except* those that you select.
Alert Filter	
Minor alert: packet loss threshold crossed?	Select **Yes** to monitor the number of minor alerts generated when packet loss (LRA-Loss Rate Average) exceeds the threshold you set in Element Manager. The default is unselected.
Minor alert: one-way latency threshold crossed?	Select **Yes** to monitor the number of minor alerts generated when one-way latency (OWDA-One Way Delay Average) exceeds the threshold you set in Element Manager. The default is unselected.
Minor alert: round-trip latency threshold crossed?	Select **Yes** to monitor the number of minor alerts generated when round-trip latency (RTA-Round Trip Average) exceeds the threshold you set in Element Manager. The default is unselected.
Minor alert: jitter threshold crossed?	Select **Yes** to monitor the number of minor alerts generated when jitter (JA-Jitter Average) exceeds the threshold you set in Element Manager. The default is unselected.
Minor alert: R-factor threshold crossed?	Select **Yes** to monitor the number of minor alerts generated when the R-factor value (LRF-Listening R Factor) falls below the threshold you set in Element Manager. The default is unselected.
Major alert: packet loss threshold crossed?	Select **Yes** to monitor the number of major alerts generated when packet loss exceeds the threshold you set in Element Manager. The default is unselected.
Major alert: one-way latency threshold crossed?	Select **Yes** to monitor the number of major alerts generated when one-way latency exceeds the threshold you set in Element Manager. The default is unselected.
Major alert: round-trip latency threshold crossed?	Select **Yes** to monitor the number of major alerts generated when round-trip latency exceeds the threshold you set in Element Manager. The default is unselected.
Major alert: jitter threshold crossed?	Select **Yes** to monitor the number of major alerts generated when jitter exceeds the threshold you set in Element Manager. The default is unselected.
Major alert: R-factor threshold crossed?	Select **Yes** to monitor the number of major alerts generated when the R-factor value falls below the threshold you set in Element Manager. The default is unselected.
Include or exclude specific phones	You can further filter your results by monitoring vqalerts only for phones you specify in the *Phone filter* parameters. The default is Exclude. • Select **Include** to monitor vqalerts only for the selected phones. • Select **Exclude** to monitor vqalerts for all phones *except* those that you select.
Phone Filter	

Parameter	How to Set It
Enterprise Network Association Name	Provide the network name associated with the phones for which you want to monitor vqalerts. This network name identifies a grouping of phones behind a firewall.
Phone Enterprise IP address	For the phones associated with the *Enterprise Network Association Name*, provide the IP address used as the bearer path before it gets to the firewall. Separate multiple addresses with a comma. An asterisk (*) is an acceptable wildcard.

CallFailures

Use this Knowledge Script to monitor LINE (line maintenance) logs. The line maintenance subsystem generates LINE logs for specific occurrences, as detailed below. This script monitors LINE logs retrieved through telnet from the IEMS and collected by the log collector service.

You can monitor all or some of the following LINE logs, which are related to call failures:

- **LINE101**, generated when the system or the user runs a diagnostic test that fails.
- **LINE102**, generated when the system changes the line state from call processing busy (CPB) to lockout (LO). LINE 102 often indicates a facility problem.
- **LINE104**, generated when a problem occurs during call processing or when bearer path integrity issues are detected.
- **LINE105**, indicates permanent signal, usually a phone left offhook, but may be a line or equipment problem
- **LINE115**, generated at the termination of a call that is connected to the DMS switch but originated from another line.
- **LINE138**, generated when a call routes to a treatment, such as automated voice response.
- **LINE160**, generated when the called party does not answer within the ringing timeout period.

The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the database tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in a table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the database tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter. Select **Run once** on the Schedule tab to run this script in troubleshooting mode. The managed object does not collect call quality statistics unless this script is running, which could pose a problem should you want, for example, to troubleshoot a call that occurred five minutes ago. To perform troubleshooting as needed, also run CollectorHealth to start the collector services, which populate the Nortel CS2x supplemental database with data you can use for troubleshooting.

Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run CollectorHealth to start the log collector service.

Resource Object

NortelCS2x

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallFailures job fails. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the log collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the log collector service reports an error. The default is 5.
Raise event if data collector reports a transaction error?	Select **Yes** to raise an event if the log collector service reports a transaction error. The default is Yes. A transaction error affects a single record encountered during the data-collection connection. If there are many transaction errors for the same record, only the most recent transaction error is posted for each iteration of the connection.
Event severity when data collector reports a transaction error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the log collector service reports a transaction error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the log collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the log collector service reports a warning. The default is 15.
Include log details?	Select **Yes** to include log details in the events raised by this script. Leave this parameter unselected to suppress log details. When you select Yes, an event includes the following columns: • Severity • Report Name • Report Number • Report Time • SequenceSS (a unique identifier for a log) • SequenceDD (a unique identifier for a log) • Event Type • Event ID • Report Details
Maximum table size	If you selected Yes for *Include log details?*, specify the maximum number of rows of log detail that you want to return in events raised by this script. The default is 25 rows.
Troubleshooting	
Select call disconnect time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **Note** This parameter is valid only when you select **Run once** on the Schedule tab.
Log Filter	

Parameter	How to Set It
Include or exclude specific Logs	Use this parameter to filter the Logs you monitor. • Select **Include only** to monitor only Logs that contain the descriptive text you provide in the *Failure log description text* parameter. • Select **Exclude** to monitor all Logs except those that contain the descriptive text you provide in the *Failure log description text* parameter. The default is Exclude.
Failure log description text	Provide descriptive text that identifies the Logs you want to include in or exclude from monitoring, such as a location or an event ID.
Monitor Number of LINE Logs	
Event Notification	
Raise event if number of LINE logs exceeds threshold?	Select **Yes** to raise an event if the number of all LINE logs generated exceeds the threshold you set. The default is Yes. Enable this parameter to monitor all LINE logs: LINE101, LINE102, LINE104, LINE105, LINE115, LINE138, and LINE160. Use the LINE-specific parameters to monitor individual LINE logs.
Threshold - Maximum number of LINE logs	Specify the maximum number of LINE logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE logs exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of LINE logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE101 Logs	
Event Notification	
Raise event if number of LINE101 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE101 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE101 logs	Specify the maximum number of LINE101 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE101 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE101 logs exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of LINE101 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE101 logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE102 Logs	
Event Notification	
Raise event if number of LINE102 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE102 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE102 logs	Specify the maximum number of LINE102 logs that can be generated before an event is raised. The default is 100 logs.

Parameter	How to Set It
Event severity when number of LINE102 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE102 logs exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of LINE102 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE102 logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE104 Logs	
Event Notification	
Raise event if number of LINE104 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE104 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE104 logs	Specify the maximum number of LINE104 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE104 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE104 logs exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of LINE104 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE104 logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE105 Logs	
Event Notification	
Raise event if number of LINE105 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE105 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE105 logs	Specify the maximum number of LINE105 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE105 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE105 logs exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of LINE105 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE105 logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE115 Logs	
Event Notification	
Raise event if number of LINE115 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE115 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE115 logs	Specify the maximum number of LINE115 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE115 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE115 logs exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for number of LINE115 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE115 logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE138 Logs	
Event Notification	
Raise event if number of LINE138 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE138 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE138 logs	Specify the maximum number of LINE138 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE138 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE138 logs exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of LINE138 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE138 logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE160 Logs	
Event Notification	
Raise event if number of LINE160 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE160 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE160 logs	Specify the maximum number of LINE160 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE160 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE160 logs exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of LINE160 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE160 logs generated during the monitoring period. The default is Yes.

CallQuality

Use this Knowledge Script to monitor end-of-call voice quality statistics. This script raises an event when a monitored statistic exceeds or falls below the threshold you set. In addition, this script generates data streams for all monitored statistics. Event messages present call quality statistics for both legs of a call, from the sending and receiving phones, on a single line in the event detail, if data for both legs is available.

This script monitors the QoS Collector Application records that the CBM pushes to the QoS file collector service, as well as the QoS syslog records sent by the CICM Element Manager to the QoS syslog collector service:

MOS (Mean Opinion Score)

The quality of a VoIP transmission based on the "mouth-to-ear" characteristics of a speech path. A MOS of 5 is considered excellent. A MOS of 1 is unacceptably bad.

R-Value

Call quality value derived from delays and equipment impairment factors. An R-Value can be mapped to an estimated MOS. R-Values range from 100 (excellent) to 0 (poor).

Jitter

Also called delay variation, jitter is the mean deviation of the difference in packet spacing between the receiving phone and the sending phone.

Latency

The time taken for a packet of data to be sent by a phone, travel, and be received by another phone.

Packet loss

Percentage of packets lost or dropped between the sending and receiving phone.

Note

You can trigger NetIQ Vivinet Diagnostics to diagnose the problem when monitored voice quality statistics exceed the thresholds you set. For more information, see "Triggering Call and Phone Quality Diagnoses" on page 3067.

The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the database tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in a table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the database tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter. Select **Run once** on the Schedule tab to run this script in troubleshooting mode. AppManager does not collect call quality statistics unless this script is running, which could pose a problem should you want, for example, to troubleshoot a call that occurred five minutes ago. To perform troubleshooting as needed, also run CollectorHealth to start the collector services, which populate the Nortel CS2x supplemental database with data you can use for troubleshooting.

Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run CollectorHealth to start the QoS syslog collector service.

Resource Object

NortelCS2x IEMS

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CallQuality job. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the collector services report an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the collector services report an error. The default is 5.
Raise event if data collector reports a transaction error?	Select **Yes** to raise an event if the collector services report a transaction error. The default is Yes. A transaction error affects a single record encountered during the data-collection connection. If there are many transaction errors for the same record, only the most recent transaction error is posted for each iteration of the connection.
Event severity when data collector reports a transaction error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the collector services report a transaction error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the collector services report a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the collector services report a warning. The default is 15.

Parameter	How to Set It
Include call details?	Select **Yes** to include call details in the events raised by this script. Leave this parameter unselected to suppress call details. When you select Yes, an event message includes the following columns: • Listening Avg MOS • Listening Avg R-Value • Average Jitter (ms) • Average Latency (ms) • Lost Packets (%) • Transmit Codec • Receive Codec • IP Address • MAC Address • Equipment • Connect Time • Disconnect Time • Duration (seconds)
Maximum table size	If you selected Yes for *Include call details?*, specify the maximum number of rows of call detail to return in events raised by this script. The default is 25 rows.
Raise event if no records found?	Select **Yes** to raise an event if there are no call quality records to monitor in the Nortel CS2x supplemental database. Note that this does not mean there are no records with call quality data, but that there are no records at all. The default is unselected.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no call quality records were found. The default is 25.
Monitor Settings	
Perform traceroute and launch Vivinet Diagnostics when voice quality alert is received?	Select **Yes** to send a traceroute request to the CICM Element Manager and to launch Vivinet Diagnostics to diagnose the problem if vqalerts are received. The default is Yes.
Length of time to wait for traceroute responses	Specify the maximum length of time that the CallQuality job should wait for a response to traceroute requests to the CICM Element Manager. The CallQuality job will fail if the response time is longer than you specify. The default is 120 seconds.
Query Filters	No matter how many calls match the filters you select, an event message displays only the first 50 calls.
Minimum duration	Use this parameter to filter out records whose call duration is less than the value you specify. Accept the default of 0 seconds to ignore the filter for minimum duration.
Maximum duration	Use this parameter to filter out records whose call duration is greater than or equal to the value you specify. Accept the default of 0 seconds to ignore the filter for maximum duration.
Troubleshooting	
Select call disconnect time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **Note** This parameter is valid only when you select **Run once** on the Schedule tab.
Monitor Average MOS	

Parameter	How to Set It
Event Notification	
Raise event if average MOS falls below threshold?	Select **Yes** to raise an event if the average MOS value falls below the threshold you set. The default is Yes.
Threshold - Minimum average MOS	Specify the lowest average MOS value that must occur to prevent an event from being raised. The default is 3.60.
Event severity when average MOS falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average MOS value falls below the threshold you set. The default is 5.
Data Collection	
Collect data for average MOS?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average MOS value during the monitoring period. The default is unselected.
Monitor Average R-Value	
Event Notification	
Raise event if average R-Value falls below threshold?	Select **Yes** to raise an event if the average R-Value falls below the threshold you set. The default is Yes.
Threshold - Minimum average R-Value	Specify the lowest average R-Value that must occur to prevent an event from being raised. The default is 70.
Event severity when average R-Value falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average R-Value falls below the threshold. The default is 5.
Data Collection	
Collect data for average R-Value?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average R-Value during the monitoring period. The default is unselected.
Monitor Average Jitter	
Event Notification	
Raise event if average jitter exceeds threshold?	Select **Yes** to raise an event if the average jitter value exceeds the threshold. The default is Yes.
Threshold - Maximum average jitter	Specify the highest average jitter value that can occur before an event is raised. The default is 60 milliseconds.
Event severity when average jitter exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average jitter value exceeds the threshold. The default is 15.
Data Collection	
Collect data for average jitter?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average amount of jitter that occurred during the monitoring period. The default is unselected.
Monitor Average Latency	
Event Notification	
Raise event if average latency exceeds threshold?	Select **Yes** to raise an event if the average latency value exceeds the threshold. The default is Yes.
Threshold - Maximum average latency	Specify the highest amount of average latency that can occur before an event is raised. The default is 400 milliseconds.
Event severity when average latency exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average latency value exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for average latency?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average amount of latency that occurred during the monitoring period. The default is unselected.
Monitor Average Packet Loss	
Event Notification	
Raise event if average packet loss exceeds threshold?	Select **Yes** to raise an event if the average packet loss value exceeds the threshold. The default is Yes.
Threshold - Maximum average packet loss	Specify the highest amount of average packet loss that can occur before an event is raised. The default is 1%.
Event severity when average packet loss exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average packet loss value exceeds the threshold. The default is 15.
Data Collection	
Collect data for average packet loss?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of average packet loss that occurred during the monitoring period. The default is unselected.

CollectorHealth

Use this Knowledge Script to start the collector services and monitor their activity and availability. This script raises an event when a collector service is unavailable and when activity falls below the threshold you set. In addition, this script generates data streams for activity and availability of the following collector services:

- Log collector service, which receives logs from the IEMS
- OM file collector service, which receives OM Reports from the IEMS
- QoS file collector service, which receives end-of-call QoS Collector Application records from the CBM
- QoS syslog collector service, which receives syslogs from the CICM Element Manager

Prerequisites

- Configure the sFTP server user name and password in AppManager Security Manager. The OM and QoS syslog collector services receive data over secure FTP (sFTP). For more information, see "Troubleshooting" on page 3046.
- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.

Resource Object

NortelCS2x Data Collector

Run only one CollectorHealth job per data collector resource.

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CollectorHealth job. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if a collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which a collector service reports an error. The default is 5.

Parameter	How to Set It
Raise event if data collector reports a transaction error?	Select **Yes** to raise an event if a collector service reports a transaction error. The default is Yes. A transaction error affects a single record encountered during the data-collection connection. If there are many transaction errors for the same record, only the most recent transaction error is posted for each iteration of the connection.
Event severity when data collector reports a transaction error	Set the severity level, from 1 to 40, to indicate the importance of an event in which a collector service reports a transaction error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if a collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which a collector service reports a warning. The default is 15.
Monitor Collector Availability	
Event Notification	
Raise event if collector service is unavailable?	Select **Yes** to raise an event if a collector service is unavailable. The default is Yes.
Event severity when collector service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which a collector service is unavailable. The default is 5.
Data Collection	
Collect data for collector service availability?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns 0 if a collector service is unavailable and 100 if a collector service is available. The default is Yes.
Remediation	
Automatically start/restart collector service?	Select **Yes** to send a start request to a collector service. The start request allows the collector service to begin collecting data and populating the supplemental database. Data collection continues until the CollectorHealth job is stopped. If the collector service stops for any reason, it is restarted. The default is Yes. If you disable this parameter, the CollectorHealth job passively monitors collector service requests from other Knowledge Scripts. However, the CollectorHealth job does not request any data collection.
Monitor Collector Activity	
Event Notification	
Raise event if collector activity falls below threshold?	Select **Yes** to raise an event if collector service activity falls below the threshold you set. The default is Yes.
Threshold - Minimum collector activity	Specify the minimum number of transactions a collector service must perform to prevent an event from being raised. The default is 1 transaction per monitoring period.
Event severity collector activity falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which collector service activity falls below the threshold. The default is 15.
Data Collection	
Collect data for collector activity?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of collector transactions during the monitoring period. The default is Yes.

Troubleshooting

Review the following topics for answers to questions you may have.

CollectorHealth Job Fails Password Authentication

Problem: The CollectorHealth job fails with the following error message:

```
Password authentication failed to <computer name>.
```

Cause: Most likely, the incorrect sFTP server user name and password are configured in AppManager Security Manager. The OM and QoS file collector services attempt to access the sFTP server using the user name and password configured in Security Manager. After *n* failed attempts (depending on how the switch is configured), the switch locks out the collector services and ignores subsequent login attempts.

Solution: Provide the correct user name and password in Security Manager. After the lockout expires, login succeeds and the CollectorHealth job runs successfully.

Log Collector Service Unavailable After a Power Outage

Problem: After a power outage, the CollectorHealth job raises an event indicating that the Log collector service is "unable to connect" to the IEMS.

Cause: Most likely, the IEMS service has not recovered from the power outage.

Solution: Verify the status of the IEMS service. If the service is down, issue the following command:

```
servstart iems
```

LogQuery

Use this Knowledge Script to monitor the number of logs in reports you specify. This script raises an event when the number of logs in the report exceeds the threshold you set.

This script uses the data collected by the log collector service.

The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the database tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in a table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the database tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter. Select **Run once** on the Schedule tab to run this script in troubleshooting mode. AppManager does not collect call quality statistics unless this script is running, which could pose a problem should you want, for example, to troubleshoot a call that occurred five minutes ago. To perform troubleshooting as needed, also run CollectorHealth to start the collector services, which populate the Nortel CS2x supplemental database with data you can use for troubleshooting.

Monitoring Examples

The following table provides examples of report name and report number combinations you can use to monitor specific activities. Provide the report name in the *Report name* parameter and the report number in the *Report number* parameter.

Activity	Report	Number
Equipment down	PM	102
Equipment up	PM	106

Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run CollectorHealth to start the log collector service.

Resource Object

NortelCS2x IEMS

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the LogQuery job fails. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the log collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the log collector service reports an error. The default is 5.
Raise event if data collector reports a transaction error?	Select **Yes** to raise an event if the log collector service reports a transaction error. The default is Yes. A transaction error affects a single record encountered during the data-collection connection. If there are many transaction errors for the same record, only the most recent transaction error is posted for each iteration of the connection.
Event severity when data collector reports a transaction error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the log collector service reports a transaction error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the log collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the log collector service reports a warning. The default is 15.
Include details?	Select **Yes** to include log details in the events raised by this script. Leave this parameter unselected to suppress log details. When you select Yes, an event includes the following columns: • Severity • Report Name • Report Number • Report Time • SequenceSS (a unique identifier for a log) • SequenceDD (a unique identifier for a log) • Event Type • Event ID • Report Details
Maximum table size	If you selected Yes for *Include details?*, specify the maximum number of rows of log detail that you want to return in events raised by this script. The default is 25 rows.
Troubleshooting	
Select log time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **Note** This parameter is valid only when you select **Run once** on the Schedule tab.
Report name	Provide the name of the log report you want to query.
Report number	Provide the ID number of the log report you want to query.

Parameter	How to Set It
Include or exclude specific reports	Select the filter to use when querying log reports. • Select **Include only** to use only the log report specified in the *Log report description* parameter. • Select **Exclude** to query for all log reports except the report specified in the *Log report description* parameter. The default is Exclude.
Log report filter	
Log report description	Use this parameter to further filter the logs in the report you want to query. Provide a text explanation of the log you want to include or exclude from querying. An asterisk (*) is an acceptable wildcard. For example, to filter for any log that mentions a CICM, type `*CICM*`.
Monitor Number of Logs	
Event Notification	
Raise event if number of logs exceeds threshold?	Select **Yes** to raise an event if the number of logs in the specified report exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of logs	Specify the maximum number of logs that can be in the specified report before an event is raised. The default is 100 logs.
Event severity when number of logs exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of logs in the specified report exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of line logs found in the specified report. The default is Yes.

OMQuery

Use this Knowledge Script to monitor the value of a specified field in a specified table in an OM Report. This script raises an event when the value of the specified field exceeds the threshold you set.

This script uses the data collected by the OM file collector service.

The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the database tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in a table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the database tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter. Select **Run once** on the Schedule tab to run this script in troubleshooting mode. AppManager does not collect call quality statistics unless this script is running, which could pose a problem should you want, for example, to troubleshoot a call that occurred five minutes ago. To perform troubleshooting as needed, also run CollectorHealth to start the collector services, which populate the Nortel CS2x supplemental database with data you can use for troubleshooting.

Monitoring Examples

The following table provides examples of table/field name combinations you can use to monitor specific activities. Provide the table name in the *Table name* parameter and the field name in the *Field name* parameter.

Activity	Table	Field Name
Originating line calls	LMD	NTERMATT
Terminating line calls	LMD	NORIGATT
Outgoing trunk calls	OFZ	NORIG
Incoming trunk calls	OFZ	NIN
Blocked terminations: not enough channels or network resources to complete calls	LMD	TERMBLK
Blocked originations: not enough channels or network resources to originate calls	LMD	ORIGBLK
Blocked trunk calls	OFZ	TRMBLK
Failed originations, other than blocked: bad signaling, partial dial tone, bad dial tone	LMD	ORIGFAIL
Failed terminations, other than blocked	LMD	PERCLFL
Peripheral origination denied, device overload	PMOVLD	PORGDENY
Peripheral termination denied, device overload	PMOVLD	PTRMDENY
Calls lost due to equipment being down	PM	PMSBTCO

Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run CollectorHealth to start the OM file collector service.

Resource Object

NortelCS2x IEMS

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OMQuery job fails. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the OM file collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OM file collector service reports an error. The default is 5.
Raise event if data collector reports a transaction error?	Select **Yes** to raise an event if the OM file collector service reports a transaction error. The default is Yes. A transaction error affects a single record encountered during the data-collection connection. If there are many transaction errors for the same record, only the most recent transaction error is posted for each iteration of the connection.
Event severity when data collector reports a transaction error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OM file collector service reports a transaction error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the OM file collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OM file collector service reports a warning. The default is 15.
Include details?	Select **Yes** to include OM Report details in the events raised by this script. Leave this parameter unselected to suppress details. When you select Yes, an event includes the following columns: • NumFound • Table Name • Field Name • Location
Maximum table size	If you selected Yes for *Include details?*, specify the maximum number of rows of detail that you want to return in events raised by this script. The default is 25 rows.
Troubleshooting	

Parameter	How to Set It
Select OM time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **Note** This parameter is valid only when you select **Run once** on the Schedule tab.
Table name	Provide the name of the table that you want to query in the OM Report.
Field name	Provide the alpha-numeric identifier of the field in the table that you want to query. **Hints** • When running this script in monitoring mode, provide only one field name for this parameter. • When running this script in troubleshooting mode, leave this parameter blank.
Include or exclude specific locations	Select the IEMS systems for which you want to query OM Reports. • Select **Include only** to query only the OM Reports from the system specified in the *Location* parameter. • Select **Exclude** to query OM Reports for all systems except the system specified in the *Location* parameter. The default is Exclude.
Location	Provide the name of the IEMS system that you want to include or exclude from the querying of OM Reports.
Monitor OM Value	
Event Notification	
Raise event if value of OM Report exceeds threshold?	Set to **Yes** to raise an event if the value of the specified field in the OM Report exceeds the threshold you set. The default is Yes.
Threshold - Maximum value of OM Report	Indicate the maximum value allowed in the specified field in the OM Report. An event is raised if the value exceeds the threshold you set. The default is 100 units. **Note** The value of the data stream generated by the script is a sum of the contents of all instances of the field you identified in the *Field name* parameter. AppManager applies the threshold to the data stream value.
Event severity when value of OM Report exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the value of the specified field in the OM Report exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for value of OM Report?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the value of the specified field in the OM Report. The default is Yes.

PhoneDiagnostic

Use this Knowledge Script to invoke NetIQ Vivinet Diagnostics to diagnose call quality between the phone on which you run this script and another specified phone. This script's sole purpose is to invoke Vivinet Diagnostics on-demand, without waiting for a problem to be identified by the CallQuality or PhoneQuality Knowledge Script jobs.

This Knowledge Script job raises an event that launches the Action_DiagnoseVoIPQuality Knowledge Script, which in turn invokes Vivinet Diagnostics. For more information, see "Triggering Call and Phone Quality Diagnoses" on page 3067.

Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the Nortel CS2x supplemental database.
- Run CollectorHealth to start the QoS syslog collector service to populate the supplemental database with call quality data.
- Run RetrieveConfigData to populate the supplemental database with phone configuration data.
- Run AddPhone to add the phones you want to monitor to the AppManager console.

Resource Object

NortelCS2x Station Object

Default Schedule

By default, this script runs on an asynchronous schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the PhoneDiagnostic job fails. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the QoS syslog collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QoS syslog collector service reports an error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the QoS syslog collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QoS syslog collector service reports a warning. The default is 15.
Monitor Settings	

Parameter	How to Set It
Length of time to wait for traceroute responses	Specify the maximum length of time that the PhoneDiagnostic job should wait for a response to traceroute requests to the CICM Element Manager. The PhoneDiagnostic job will fail if the response time is longer than you specify. The default is 120 seconds.
Far End (Remote) Phone Settings	
Select remote phone by	Select the category by which you want to choose the phone you want to monitor. Select **Terminal**, **DN**, or **IPAddress**. The default is DN.
Selection criteria	Based on your selection in *Select remote phone by*, provide details for the phone you want to monitor. Vivinet Diagnostics diagnoses call quality between this phone and the phone on which you run this script. • *If you selected Terminal*, provide the terminal address of the phone you want to monitor. • *If you selected DN*, provide the Directory Number of the phone you want to monitor • *If you selected IPAddress*, provide the IP address of the phone you want to monitor.

PhoneInventory

Use this Knowledge Script to create an inventory of the phones configured for a CICM Element Manager.

You choose both the search criteria for the inventory report and the location of the output folder. The inventory report is written to the computer on which the AppManager agent is running, unless you specify a UNC path: \\`servername\sharename\directoryname\filename`. If you specify a UNC path, ensure the `NetIQmc` service is running as an account that has proper permissions on the UNC path.

Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run RetrieveConfigData to populate the supplemental database with phone configuration information.

Resource Object

NortelCS2x

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the PhoneInventory job fails. The default is 5.
Raise event if phone inventory succeeds?	Select **Yes** to raise an event when a phone inventory report is successfully generated. The default is Yes.
Event severity when phone inventory succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a phone inventory report is successfully generated. The default is 25.
Raise event if no records found?	Set to **Yes** to raise an event when the PhoneInventory job finds no phones based on the criteria you selected. The default is Yes
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the PhoneInventory job found no phones based on the criteria you selected. The default is 25.
Search Options	

Parameter	How to Set It
Select phones by	Select the filter by which you want to select the phones for the inventory report. Choose one of the following: • Node • Terminal • DN (Directory Number, the default) • Station Type • Network Name • Network ID • IP Address
Selection criteria	Provide the selection criteria for the phones to include in the inventory report. You can specify the actual item or you can specify a pattern by using the * wildcard. For example, to monitor all the phones in the ADM building, type `ADM*`. You can enter multiple criteria by separating each item with a comma. For example: `ADM0009A*,ADM0009B*` The criteria you enter must be of the same type as the *Select phones by* parameter. So if *Select phones by* is Terminal, then the criteria must be terminal names or patterns. If *Select phones by* is DN, then the criteria must be phone extension numbers. **Note** Only the following characters are acceptable in this field: • Numbers • Uppercase and lowercase letters • Periods • Commas • Asterisks (*) • Underscores • Spaces
List only phones with status of	To further filter the list of phones, select a status. Only phones of this status type, matching the criteria you specified in *Selection criteria* and *Select phones by*, are included in the inventory report. Choose one of the following: • Any • Logged In • Logged Out
Result File Options	
Full path to output folder for result file	Type the full path or a UNC path to a location on the agent computer in which to save the inventory .csv file. The default path is `c:\Program Files\NetIQ\Temp\NetIQ_Debug\PhoneInventory.csv`
Sort by	Select **Name** to sort the contents of the inventory report in order by phone name, specifically by the “node” column and then by the “terminalid” column. Select **DN** to sort the contents of the inventory report in order by Directory Number, specifically by the “ud_pDN” column (Primary Directory Number) column. The default is DN.

PhoneQuality

Use this Knowledge Script to monitor real-time voice quality statistics from active calls on IP phones. This script raises one event per call if monitored statistics exceed or fall below the threshold you set. In addition, this script generates data streams for each monitored statistic.

This script monitors the mid-call QoS records for the Phase 2 IP phones on which you run this script. The QoS syslog collector service receives those records from the Call Server and pushes those records to the supplemental database.

MOS (Mean Opinion Score)

Represents the quality of a VoIP transmission by factoring in the "mouth-to-ear" characteristics of a speech path. A MOS of 5 is considered excellent; a MOS of 1 is unacceptably bad.

R-Value

Call quality value derived from delays and equipment impairment factors. An R-Value can be mapped to an estimated MOS. R-Values range from 100 (excellent) to 0 (poor).

Jitter

Also called delay variation, jitter is the mean deviation of the difference in packet spacing between the calling phone and the called phone.

Latency

The time taken for a data packet to be sent by a phone, travel, and be received by another phone.

Packet loss

Packets lost or dropped between the calling and called phone

Note

You can trigger NetIQ Vivinet Diagnostics to diagnose the problem when monitored voice quality statistics exceed the thresholds you set. For more information, see "Triggering Call and Phone Quality Diagnoses" on page 3067.

Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the Nortel CS2x supplemental database.
- Run RetrieveConfigData to populate the supplemental database with phone configuration data.
- Run AddPhone to add the phones you want to monitor to the AppManager console.
- Run CollectorHealth to start the QoS syslog collector service.

Resource Object

NortelCS2x Station Object

Default Schedule

By default, this script runs on an asynchronous schedule.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the PhoneQuality job. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the QoS syslog collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QoS syslog collector service reports an error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the QoS syslog collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QoS syslog collector service reports a warning. The default is 15.
Monitor Settings	
Data collection interval for voice quality metrics	Specify how often the PhoneQuality script should collect phone quality statistics from the supplemental database. The default is 30 seconds, the minimum is 15 seconds, and the maximum is 1000000 seconds.
Perform traceroute and launch Vivinet Diagnostics when voice quality alert is received?	Select **Yes** to send a traceroute request to the CICM Element Manager and to launch Vivinet Diagnostics to diagnose the problem if vqalerts are received. The default is Yes.
Length of time to wait for traceroute responses	Specify the maximum length of time that the PhoneQuality job should wait for a response to traceroute requests to the CICM Element Manager. The PhoneQuality job will fail if the response time is longer than you specify. The default is 120 seconds.
Monitor Interval MOS	
Event Notification	
Raise event if interval MOS falls below threshold?	Select **Yes** to raise an event if the MOS value during the data collection interval falls below the threshold you set. The default is Yes.
Threshold - Minimum interval MOS	Specify the minimum MOS value that must occur during the data collection interval to prevent an event from being raised. The default is 3.60.
Event severity when interval MOS falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MOS value during the data collection interval falls below the threshold. The default is 5.
Data Collection	
Collect data for interval MOS?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the MOS value during the data collection period. The default is Yes.
Monitor Interval R-Value	
Event Notification	
Raise event if interval R-Value falls below threshold?	Select **Yes** to raise an event if the R-Value during the data collection interval falls below the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold - Minimum interval R-Value	Specify the lowest R-Value that must occur during the data collection interval to prevent an event from being raised. The default is 70.
Event severity when interval R-Value falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the R-Value during the data collection interval falls below the threshold. The default is 5.
Data Collection	
Collect data for interval R-Value?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the R-Value during the data collection interval. The default is unselected.
Monitor Interval Jitter	
Event Notification	
Raise event if interval jitter exceeds threshold?	Select **Yes** to raise an event if the jitter value during the data collection interval exceeds the threshold you set. The default is Yes.
Threshold - Maximum interval jitter	Specify the highest jitter value that can occur during the data collection interval before an event is raised. The default is 60 milliseconds.
Event severity when jitter exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the jitter value exceeds the threshold. The default is 15.
Data Collection	
Collect data for interval jitter?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of jitter that occurred during the data collection interval. The default is unselected.
Monitor Interval Latency	
Event Notification	
Raise event if interval latency exceeds threshold?	Select **Yes** to raise an event if the latency value during the data collection interval exceeds the threshold you set. The default is Yes.
Threshold - Maximum interval latency	Specify the highest amount of latency that can occur during the data collection interval before an event is raised. The default is 400 milliseconds.
Event severity when interval latency exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the latency value during the data collection interval exceeds the threshold. The default is 15.
Data Collection	
Collect data for interval latency?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of latency that occurred during the data collection interval. The default is unselected.
Monitor Interval Packet Loss	
Event Notification	
Raise event if interval packet loss exceeds threshold?	Select **Yes** to raise an event if the packet loss value during the data collection interval exceeds the threshold. The default is Yes.
Threshold - Maximum interval packet loss	Specify the highest percentage of packet loss that can occur during the data collection interval before an event is raised. The default is 1%.
Event severity when interval packet loss exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the packet loss value during the data collection interval exceeds the threshold. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for interval packet loss?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of packet loss that occurred during the monitoring period. The default is unselected.

RemovePhone

Use this Knowledge Script to remove IP phones (stations) from the AppManager console. This Knowledge Script is not available for use if you never used AddPhone to add an IP station.

When this Knowledge Script job runs successfully, the resource object for an IP station is deleted from the AppManager console. The job itself is not deleted, nor is the event that the job creates because the event is associated with the parent object: `NortelCS2x:<computer name>` object. However, you can set a global preference to ensure that an event is deleted when the associated object is deleted.

To delete associated events:

1. From the File menu, select **Preferences**.
2. Click **Repository**, and then click **Event**.
3. Select **Remove associated events when jobs are deleted**.

Tips

- When you run this script, verify your selected phones in the Objects tab to avoid removing a phone that you want to keep.
- Before attempting to remove a phone, stop any monitoring jobs that are running on the phone.

Resource Object

NortelCS2x Station Object

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the failure of the RemovePhone job. The default is 5.
Event Notification	
Raise event if phones are removed successfully?	Select **Yes** to raise an event if the selected IP stations are successfully removed from AppManager console. The default is Yes.
Event severity when phones are removed successfully	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the selected IP stations are successfully removed from the AppManager console. The default is 25.

RetrieveConfigData

Use this Knowledge Script to retrieve station configuration information from individual CICM Element Managers. This script stores the configuration information in the Nortel CS2x supplemental database, where it can be monitored by the PhoneInventory and PhoneDiagnostic Knowledge Scripts.

Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Configure the CICM Element Manager user name and password in AppManager Security Manager.

Resource Object

NortelCS2x

Default Schedule

By default, this script runs once every day at 3 AM, so as to perform CPU-intensive functions at a time when Element Managers are least busy.

To populate the supplemental database immediately, change the schedule to **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the failure of the RetrieveConfigData job. The default is 5.
Raise event if configuration retrieval succeeds?	Select **Yes** to raise an event if the RetrieveConfigData job successfully stores station configuration information in the Nortel CS2x supplemental database. The default is unselected.
Event severity when configuration retrieval succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which configuration information is successfully stored in the NortelCS2x supplemental database. The default is 25.

SetupSupplementalDB

Use this Knowledge Script to create the Nortel CS2x supplemental database, including the tables and stored procedures needed to store logs, OM Reports, QoS and call detail records, and station configuration information. In addition, this script creates a SQL Server job that removes old records from the supplemental database.

When you create the supplemental database, you specify how long data is retained before being deleted. AppManager automatically deletes any records older than the retention age you specify.

Understanding the Supplemental Database

The Nortel CS2x supplemental database is a Microsoft SQL Server database you create locally on the proxy agent computer or on a specified remote computer. The log, OM, QoS syslog, and QoS file collector services receive data from the IEMS, the CICM, the CBM, and the Call Server, and then store that data in the supplemental database.

- The CollectorHealth Knowledge Script verifies that collectors are receiving data and starts the process by which the collectors push their data to the supplemental database.
- The CallActivity, CallFailures, CallQuality, LogQuery, and OMQuery, and PhoneQuality Knowledge Scripts query the supplemental database for the data you specify.
- The RetrieveConfigData Knowledge Script populates the supplemental database with station information used by the PhoneInventory and PhoneDiagnostic Knowledge Scripts.

To create and use the supplemental database:

1. **Create the database**. Create one Nortel CS2x supplemental database per office supported by a Communication Server solution. You can create the supplemental database when you run Discovery_NortelCS2x or SetupSupplementalDB.
2. **Populate the database**. Run CollectorHealth and RetrieveConfigData to populate the Nortel CS2x supplemental database.
3. **Monitor the data in the database**. Depending on your monitoring objectives, run the following scripts to analyze the data in the database.
   - CallActivity monitors active and completed calls.
   - CallFailures monitors LINE (line maintenance) logs.
   - CallQuality monitors end-of-call voice quality statistics: jitter, latency, lost data, MOS, and R-Value.
   - LogQuery monitors logs in specified log reports.
   - OMQuery monitors specified fields in the OM Report.
   - PhoneDiagnostic invokes NetIQ Vivinet Diagnostics to diagnose call quality between two phones.
   - PhoneInventory creates an inventory of the phones configured in a CICM Element Manager.
   - PhoneQuality monitors real-time, mid-call voice quality statistics from active calls on IP phones.

Resource Object

NortelCS2x IEMS

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SetupSupplementalDB job. The default is 5.
Raise event if database setup succeeds?	Select **Yes** to raise an event if creation of the Nortel CS2x supplemental database is successful. The default is unselected.
Event severity when database setup succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the success of the creation of the Nortel CS2x supplemental database. The default is 25.
Number of days to keep supplemental database records	Specify the number of days you want to keep records in the Nortel CS2x supplemental database. Data older than that is discarded. The default is 14 days.
SQL Server computer name	Specify the hostname or IP address of the remote SQL Server computer on which you want to create the Nortel CS2x supplemental database. Leave this parameter blank to create the supplemental database on the proxy agent (local) computer. For either a remote or local supplemental database, configure the SQL Server user name and password in AppManager Security Manager. For a remote supplemental database, set up the remote SQL Server computer.

Parameter	How to Set It
SQL Server instance name	Specify the name of the SQL Server instance on the computer on which you want to create the Nortel CS2x supplemental database. Leave this parameter blank to accept the default instance name.
Start pruning job on supplemental database?	**For all supported versions of SQL Server, except SQL Server 2005 Express**: Set to **Yes** to create a SQL job that deletes data from the supplemental database. The SQL job runs every night. Data is deleted from the supplemental database based on the value you specify in the *Number of days to keep call detail records* parameter. The default is Yes. **For SQL Server 2005 Express**: Set to **No**. The pruning job is not supported for SQL Server 2005 Express. **To manually delete data from the supplemental database**: 1. Run the following stored procedure from a command line: `osql -E -S <sql server> -n -d <database> -Q "exec dbo.Task_NortelCS2x_Pruning"` where <`sql server`> is the name of the server that hosts the supplemental database, and where <`database`> is the name of the supplemental database. For example: `osql -E -S SuppDBNortelCS2x -n -d NortelCS2x_S8300-Cluster -Q "exec dbo.Task_NortelCS2x_Pruning"` 2. Configure a Windows Scheduled Task to schedule pruning at an interval of your choosing. The process for configuring a Windows Scheduled Task varies according to your version of Microsoft Windows. Consult your Windows documentation for more information.

Recommended Knowledge Script Group

The following Knowledge Scripts in the AppManager for Nortel CS2x module are members of the NortelCS2x recommended Knowledge Script Group (KSG).

- CallActivity
- CallFailures
- CallQuality
- CollectorHealth

You can find the NortelCS2x KSG on the RECOMMENDED tab of the Knowledge Script pane of the Operator Console.

All the scripts in the KSG have their parameters set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab, and then run the NortelCS2x group on a Nortel CS2x resource.

Run the KSG from the Master view, not the NortelCS2x view. In order to use the Discovery_NortelCS2x Knowledge Script in a monitoring policy, the view must include root objects, which are not visible in the NortelCS2x view.

The NortelCS2x KSG enables a "best practices" usage of AppManager for monitoring your Nortel CS2x environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView. For more information, see "About Policy-Based Monitoring" in the AppManager Help.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the NortelCS2x tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the NortelCS2x tab are not affected.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the NortelCS2x KSG and want to restore it to its original form, you can reinstall AppManager for Nortel CS2x on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\NortelCS2x` directory.

Triggering Call and Phone Quality Diagnoses

You can use NetIQ Vivinet Diagnostics to diagnose problems identified by NortelCS2x Knowledge Scripts.

Using the existing methodology of launching an Action script based on an event, AppManager can launch Action_DiagnoseVoIPQuality to trigger Vivinet Diagnostics in the following instances. The Action script runs by default only if Vivinet Diagnostics 2.3 or later is installed on the computer on which the script is running.

- To diagnose the problem for events raised by the CallQuality and PhoneQuality Knowledge Scripts.
- You can use the PhoneDiagnostic Knowledge Script to trigger Vivinet Diagnostics on demand, rather than waiting for a problem to be identified by the CallQuality and PhoneQuality Knowledge Scripts.

You can also use the CallAlert Knowledge Script to trigger Vivinet Diagnostics to diagnose the problems indicated by vqalerts.

To trigger Vivinet Diagnostics:

1. When setting parameter values for the CallQuality, PhoneQuality, or PhoneDiagnostic Knowledge Scripts, click the **Action** tab. Action_DiagnoseVoIPQuality is selected by default.
2. Click **Properties** and enter values for all parameters for Action_DiagnoseVoIPQuality.
3. Click **OK** to run the CallQuality, PhoneQuality, or PhoneDiagnostic Knowledge Script jobs.

The event message for the Action_DiagnoseVoIPQuality job provides a hyperlink to a .dgv file, which is the Diagnosis. Click the link to view the Diagnosis in the Vivinet Diagnostics console. For more information, see the *User Guide for Vivinet Diagnostics* and the Help for the Action_DiagnoseVoIPQuality Knowledge Script.

Chapter 53
NT Knowledge Scripts

The NT category provides Knowledge Scripts for monitoring Microsoft Windows servers and workstations. This category also includes reporting scripts you can use to create meaningful reports about your Microsoft Windows servers and workstations.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ConfigRemoteServiceDown	Loads the parameters specific to a local monitored computer and makes them available to the RemoteServiceDownLR Knowledge Script.
ConfigServiceDown	Loads the parameters specific to a local monitored computer and makes them available to the ServiceDownLR Knowledge Script.
CpuByProcess	Monitors CPU usage for each process and the total CPU usage for all processes.
CpuLoaded	Monitors total CPU usage and queue length to determine CPU load.
CpuResource	Monitors user CPU, the number of active processes, the number of threads, and the number of interrupts per second.
DiskSpace	Monitors logical drives for the percentage of disk space used, the amount of free space in megabytes, and the percentage of disk growth.
DNSConnectivity	Checks connectivity between a managed computer and its DNS server.
FailedLogon	Monitors the number of failed non-interactive logon attempts, for example, failed `net use` attempts, since the last interval.
FileChanged	Checks for changes to a specified file in the last monitoring interval.
FilesCompare	Compares the size, time stamp, and attributes of two files.
FileSizeSum	Monitors the total size of two specified files.
FilesOpen	Monitors the number of open files that were opened remotely, for example, by a user who remotely logged onto the computer.
FindFiles	Monitors logical drives for files that match your filtering criteria.
FolderFileCount	Monitors folders for the number of files that match your filtering criteria.
FolderSize	Monitors the size of folders containing files matching your filtering criteria.

Knowledge Script	What It Does
IntervalCounter	Monitors the change in any performance monitor counter.
LogicalDiskStats	Monitors logical disk transfers, disk reads, disk writes, operation time, and queue length.
MemByProcess	Monitors memory use for each process and total memory usage for all processes.
MemUtil	Monitors physical memory, virtual memory, and the paging files.
NetSession	Lists the network sessions connected to a computer.
NetworkBusy	Monitors the traffic on the network interface cards on a Windows computer.
PagingHigh	Monitors paging activity per second.
PhysicalDiskStats	Monitors physical disk transfers, disk reads, disk writes, operation time, and queue length.
PortHealth	Checks whether system ports are working properly.
PrinterHealth	Checks for print job problems, such as a paused or jammed printer, and the printer queue length.
PrinterQueue	Monitors a printer's queue length.
ProcessDown	Determines whether specified processes are running.
Processes	Monitors the number of processes.
ProcessUp	Checks whether a specified process is running and, optionally, terminates the process.
RegistryChange	Monitors changes in the registry.
RemoteServiceDown	Detects if any service on a remote computer is down.
RemoteServiceDownLR	Using parameters you specified with the ConfigRemoteServiceDown Knowledge Script, this script runs on a group of computers to detect whether services on remote computers are down.
Report_CPULoad	Generates a detailed report about CPU usage and queue length.
Report_CPULoadSummary	Generates a summary report about CPU usage and queue length.
Report_CPUResource	Generates a detailed report about the use of CPU resources, including the number of active processes, threads, and interrupts per second, and the utilization of CPU resources in user mode.
Report_CPUResourceSummary	Generates a summary report about the use of CPU resources.
Report_CPUUsageofProcessesSummary	Generates a summary report about CPU usage per named process, and total CPU usage by all named processes.
Report_FilesOpen	Generates a report about the number of files open during a specified period.
Report_LogicalDiskAvailSummary	Generates a summary report about the available space (in MB) for a logical disk.
Report_LogicalDiskUsageSummary	Generates a summary report about the percentage of disk space used and the amount of free space.
Report_MemoryUtilization	Generates a detailed report about the use of physical and virtual memory, and paging files.
Report_MemoryUtilizationSummary	Generates a summary report about the use of physical and virtual memory, and paging files.

Knowledge Script	What It Does
Report_NetworkBusy	Generates a report about the use of bandwidth on network interface cards.
Report_PagingHigh	Generates a report about the number of reads and writes per second to the page file.
Report_PhysicalDiskIO	Generates a report about the number of reads, writes, and transfers per second for a physical disk.
Report_PhysicalDiskQueueLength	Generates a report about physical disk queue length.
Report_PrinterHealth	Generates a report about print job problems and printer queue length.
Report_Process	Generates a report about the number of processes running during a specified period.
Report_TopCPUProcs	Generates a report about the total CPU used by all processes and which processes consume the most CPU resources.
Report_TopMemoryProcs	Generates a report about the total memory used by all processes and which processes consume the most memory.
RunAwayProcesses	Detects runaway processes by sampling CPU usage.
ServerBusy	Monitors the Windows server activity for network clients.
ServerBytes	Monitors the number of bytes per second transferred to and from a target computer.
ServerError	Monitors the number of sessions that errored out during the monitoring interval.
ServerTimeout	Monitors the number of sessions that timed out during the monitoring interval.
ServiceChange	Detects changes to the status and start type for Windows services.
ServiceDown	Monitors the stopped and started status of Microsoft Windows services and, optionally, starts services that are stopped.
ServiceDownLR	Using parameters you specified with the ConfigServiceDown Knowledge Script, this script can run on a group of computers to detect whether specified services are down and if so, optionally restart them.
ServiceHung	Checks whether any Windows services are hung.
ServiceRemove	Detects if any Windows services are added or removed in the monitoring interval.
SharedFiles	Monitors open network shared files.
SystemUpTime	Tracks the number of hours a computer has been operational since it was last rebooted.
TopCpuProcs	Monitors total CPU used by all processes and which processes consume the most CPU resources.
TopMemoryProcs	Monitors the total memory used by all processes and which processes consume the most memory.
TrustRelationship	Tests the domain trust relationship from a trusting domain to specified trusted domains.
UnixRemoteProcessDown	Monitors applications on remote UNIX computers where you cannot easily install a UNIX agent.

ConfigRemoteServiceDown

Use this Knowledge Script to set parameter values in the local repository of the computer where you run the script. The values are used by the RemoteServiceDownLR script when it runs on that computer.

Using this pair of scripts, you can set up the computers in a group so that when the RemoteServiceDownLR script runs on the group, it can run with different parameter values on each computer. This is particularly useful for enforcing monitoring policies.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event when job completes?	Set to **y** to raise an event when the job completes, with or without errors. The default is y.
List of computers	Specify one or more computers to monitor, separating each computer name with a comma (,) and no space.
Full path to file with a list of computers	Specify the full path to and name of a text file containing a list of computers. Put each computer on a separate line; no commas or spaces. The job supports a maximum file size of 32KB. If the file size exceeds 32KB, the job stops and raises an error event message: `Out of string space`.
List of services	Specify the name of one or more services to monitor, separating each name with a comma (,) and no space. The default is `NetIQmc`.
Event severity when job completes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ConfigRemoteServiceDown job completes, with or without errors. The default is 25 (blue event indicator).

ConfigServiceDown

Use this Knowledge Script to set parameter values in the local repository of the computer on which you run the script. The values are used by the ServiceDownLR script when it runs on that computer. Using this pair of scripts, you can set up the computers in a group so that when the ServiceDownLR script runs on the group, it can run with different parameter values on each computer. This is particularly useful for enforcing monitoring policies.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event when job completes?	Select **Yes** to raise an event when the job completes, with or without errors. The default is Yes.
List of services	Specify one or more services to monitor. Use an asterisk (*) to monitor all "automatic" services. Use a comma to separate multiple service names. The default is `EventLog`.
List of excluded services	Specify one or more services to exclude from monitoring. Use an asterisk (*) to exclude all "automatic" services. Use a comma to separate multiple service names.
Event severity when job completes	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ConfigServiceDown job completes, with or without errors. The default is 25 (blue event indicator).

CpuByProcess

Use this Knowledge Script to monitor whether specified processes have exceeded CPU thresholds. This script monitors CPU usage for each named process, as well as the total CPU usage for all named processes.

To determine CPU usage, this script checks the percentage of processor time that the threads for each process used to execute instructions.

If a process is not found, the script assumes that the process is not running, and reports zero as the CPU result.

Notes

- This script does not detect invalid process names. If you enter an invalid process name, the script assumes that the process is not running, and reports zero as the CPU result.
- If the CPU usage for the named processes exceeds the threshold limit, an event is raised. However, this is not applicable for Windows System Idle Process. The System Idle Process indicates the percentage of idle CPU resources. If no applications are running, this process indicates a high idle capacity. The high percentage exceeds the threshold and raises an event indicating that the System Idle Process consumes high CPU resources. You can safely ignore this event message because the high percentage refers to the high idle capacity and not high CPU usage.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Create event for each process that exceeds the threshold?	Select **Yes** to raise an event if any individual process exceeds the CPU usage threshold you specify. The default is Yes.
Severity -- Individual process CPU high	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 8 (red event indicator).
Create event if the sum of all processes exceeds the threshold?	Select **Yes** to raise an event if the CPU usage by all processes exceeds the threshold you specify. The default is Yes.
Severity -- Total process CPU high	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage for all processes exceeds the threshold. The default is 15 (yellow event indicator).

Description	How to Set It
Severity -- Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CpuByProcess job fails unexpectedly. The default is 5 (red event indicator).
Data Collection	
Collect data for each process?	Select **Yes** to collect data for charts and reports, for each process you monitor. The default is unselected.
Collect data for all processes?	Select **Yes** to collect data for charts and reports, for all processes you monitor. The default is unselected.
Monitoring	
Processes	Specify the names of the processes you want to monitor. Separate the names with commas (,) and no spaces.
Maximum threshold for CPU for each process	Specify the maximum CPU usage allowed for *each* monitored process before an event is raised. The default is 60%.
Maximum threshold for CPU for all processes	Specify the maximum CPU usage allowed for *all* monitored processes before an event is raised. The default is 95%.

CpuLoaded

Use this Knowledge Script to monitor total CPU usage and queue length to determine whether the CPU is overloaded. This script raises an event when CPU usage and CPU queue length values exceed the thresholds you set.

Resource Objects

CPU folder or any individual CPU icon (for multiprocessor systems)

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CpuLoaded job fails. The default is 5 (red event indicator).
Raise event if total system CPU exceeds threshold?	Select **Yes** to raise an event if total system CPU usage exceeds the threshold you set. The default is Yes. This script raises an event when the following occur: • Total system CPU exceeds the threshold AND • *Threshold - Maximum processor queue length* is exceeded OR set to 0.
Event severity when total system CPU exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which system CPU usage exceeds the threshold. The default is 10 (red event indicator).
Raise event if any individual CPU exceeds threshold?	Select **Yes** to raise an event if CPU usage for any monitored server exceeds the usage threshold you set. The default is unselected. This script raises an event when the following occur: • Individual CPU exceeds the threshold AND • *Threshold - Maximum processor queue length* is exceeded OR set to 0.
Event severity when individual CPU exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which individual CPU usage exceeds the threshold. The default is 15 (yellow event indicator).
Monitoring	
Use virtual machine performance counters if available?	Select **Yes** to monitor VMware performance counter data on virtual machines, if available, instead of physical host counters. The default is Yes. VMware performance counters do not provide processor queue length data. If you select Yes, only CPU usage data is monitored.
Thresholds	
Threshold - Maximum total system CPU	Specify the maximum total system CPU usage allowed before an event is raised. The default is 95%.
Threshold - Maximum individual CPU	Specify the maximum individual CPU usage allowed before an event is raised. The default is 98%.

Description	How to Set It
Threshold - Maximum processor queue length	Specify the maximum number of processes the CPU queue can contain before an event is raised. CPU queue length indicates how many processes are ready to run. The default is 2 processes. **Note** To ignore processor queue length and monitor only CPU usage, set this threshold to 0.
Data Collection	
Collect data for total system utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the overall percentage of CPU time used. The default is unselected. The detail data contains information about the percentage of CPU usage and the threshold for percentage of CPU usage.
Collect data for individual processor utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of CPU time used for each processor in one data stream per processor. The default is unselected. The detail data contains information about the percentage of CPU usage and the threshold for percentage of CPU usage.
Collect data for processor queue length?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of threads waiting to execute on all processors. The default is unselected. The detail data contains information about processor queue length and the threshold for processor queue length.

Example of How this Script Is Used

This script monitors both the percentage of CPU used and processor queue length. By itself, high CPU usage might not indicate a problem. Instead, consider the following factors:

- Queue length
- How you are using the computers monitored
- Your overall strategy for the environment

For example, in a **transactional** environment you can have a computer with CPU usage at 90% consistently. The computer has no room for growth, but if the queue length remains low and stable (never more than two or three threads waiting), the computer can be sized perfectly for maximum efficiency. If the queue length increases and threads are waiting, you may have a problem that needs to be addressed.

In a **batch** environment, however, you can set the script to run during off-peak hours when the batch jobs are not running. The script can raise an event if CPU usage is over 50% and any thread is waiting (queue length at 0) to ensure the computer has enough CPU headroom for batch jobs to run.

Other factors to consider are long range plans, such as the number of users you expect to support, how long you expect to support them, and how much room you need for growth. For example, you can set the CPU usage threshold lower to warn you to off-load some processing or order new systems.

Monitoring Multi-Processor Systems

On a multi-processor system, the total CPU utilization is the average percentage of time that all the processors on the system are busy executing non-idle threads. For example:

- If all processors are always busy, this is 100%.
- If all processors are 50% busy, this is 50%.
- If 25% of the processors are busy, this is 25%.

Monitoring Overall or Individual CPU Load

Monitor load for each CPU individually to gain more specific information about what is really happening on a system. For example, if you monitor overall load and see CPU usage is 100%, you do not know as much about the resource usage as seeing that CPU 0 is running at 90% and CPU 1 is running at 10%.

Handling Spikes

Because CPU and queue length are often subject to temporary spikes, set a short interval (two to five minutes), but raise an event only after thresholds are exceeded in three consecutive periods.

Collecting Data for Trend Analysis

This script can be set to collect data to help you identify usage trends for your servers. For example, if CPU usage increases, you can plan for growth. To perform this type of analysis, run a second job that collects data at a less-frequent interval.

CpuResource

Use this Knowledge Script to monitor CPU resource consumption for users, the number of active processes, the number of threads, and the number of interrupts per second. This script raises an event if a monitored value exceeds the threshold you specify.

Resource Object

CPU folder

Default Schedule

The default schedule for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if any threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. The default is n.
Maximum CPU user utilization threshold	Specify the maximum CPU usage allowed in user mode before an event is raised. The default is 90%.
Maximum number of processes threshold	Specify the maximum number of processes that can be running before an event is raised. The default is 80.
Maximum number of threads threshold	Specify the maximum number of threads that can be running before an event is raised. The default is 500.
Maximum interrupts per second threshold	Specify the maximum number of interrupts per second allowed before an event is raised. The default is 600.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

DiskSpace

Use this Knowledge Script to monitor logical drives for the percentage of disk space used, the amount of free space in megabytes, and the percentage of disk growth between iterations.

Each time it runs, this script automatically monitors all logical disks on a server and all shared drives in a cluster. The owner of the quorum disk, which determines the current state of the cluster, monitors the space on shared drives. You can override automatic monitoring by providing a specific list of drives to monitor. Also, you can provide a list of drives to exclude from monitoring.

This script raises an event if the percentage of used space exceeds the threshold you set, if the amount of free space falls below the threshold you set, or if the percentage of disk growth exceeds the threshold you set.

Note
In a cluster, this script runs on the primary node to monitor disk growth. If failover occurs, this script begins monitoring disk growth on the secondary node. The first iteration of the Knowledge Script job after failover reports the disk size of the secondary node as being the same as that of the primary node. The job begins reporting disk growth during the second and subsequent iterations after failover.

Prerequisite

To use the DiskSpace Knowledge Script, you must install the AppManager for Microsoft Windows module, version 7.6.x.0 at minimum, on your agent computers.

Resource Object

Logical disk object

Default Schedule

By default, this script runs every five minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity when job fails?	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DiskSpace job fails. The default is 5.
Raise an event if threshold is crossed?	Select **Yes** to raise an event if the amount of available disk space falls below the threshold you set, if the percentage of disk utilization exceeds the threshold you set, and if the percentage of disk growth exceeds the threshold you set. The default is Yes. When you enable this parameter, the script raises one event that details the disk usage for all monitored logical drives. **Note** If you run this script on a cluster, the script raises one event per monitored node in that cluster.

Parameter	How to Set It
Raise a separate event for individual drives?	Select **Yes** to raise an event if the amount of available disk space falls below the threshold you set or the percentage of disk utilization exceeds the threshold you set. The default is unselected. When you enable this parameter, the script raises separate events that detail the disk usage for each monitored logical drive.
Event severity when a threshold is crossed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of available disk space falls below the threshold you set or the percentage of disk utilization exceeds the threshold you set. The default is 5.
Use XML format for event message?	Select **Yes** to format event detail messages in XML. Leave this parameter unselected to format event detail messages in plain text. Events formatted in XML display results in tables. Events in plain text display results in rows of unformatted text.
Disk Space Monitoring	
Drives to monitor	If you do not want this script to automaticaly monitor all logical drives, provide a comma-separated list of the drives you want to monitor. Leave this parameter blank to automatically monitor all logical drives.
Drives to exclude	Provide a comma-separated list of the drives you do not want to monitor. This script automatically monitors all drives except those listed in this parameter. The asterisk (*) is an acceptable wildcard. For example, to exclude the C: drive and disks or mount points that begin with `\crate`, specify the following: `c:,e:\crate*` The * wildcard is valid only at the end of an expression, not in the middle or beginning of an expression.
Monitor mount points?	Select **Yes** to allow the script to monitor mount points (mapped drives). The default is Yes.
Ignore disks with minimal total size?	Select **Yes** to exclude disks of a certain size from monitoring. Use the *Threshold - Minimum disk size for monitoring* parameter to set the minimum monitoring requirement. The default is Yes.
Minimum size for disk monitoring	Specify the minimum size requirement for disk monitoring. Disks of less than *n* MB are excluded from monitoring The default is 100 MB.
Thresholds	
Global threshold - Minimum available disk space	Specify the minimum amount of disk space that must be available to prevent an event from being raised. The default is 100 MB. This threshold applies to all disks unless you provide a per-disk threshold value in the *Per-disk threshold - Minimum available disk space* parameter.
Global threshold - Maximum disk utilization	Specify the maximum percentage of disk utilization that can occur before an event is raised. The default is 90%. This threshold applies to all disks unless you provide a per-disk threshold value in the *Per-disk threshold - Maximum disk utilization in %* parameter.
Global threshold - Maximum percentage of disk growth	Specify the percentage of disk growth that can occur before an event is raised. The default is 25%. For example, if you set this parameter to 30%, this script raises an event if the size of the disk is 30% larger than it was during the previous script iteration. This threshold applies to all disks unless you provide a per-disk threshold value in the *Per-disk threshold - Maximum percentage of disk growth in %* parameter.
Apply per disk thresholds?	Select **Yes** to set different thresholds for individual disks. The default is unselected.

Parameter	How to Set It
Per-disk threshold - Minimum available disk space in MB	Specify the minimum amount of disk space that must be available on individual disks to prevent an event from being raised. Use commas to separate multiple thresholds. For example: `C:=90500,D:=550` In this example, the threshold for minimum disk space on the C: disk is 90500 MB. The threshold for the D: disk is 550 MB.
Per-disk threshold - Maximum disk utilization in %	Specify the maximum percentage of disk utilization that can occur on individual disks before an event is raised. Use commas to separate multiple thresholds. For example: `C:=50,D:=80` In this example, the threshold for maximum disk utilization on the C: disk is 50%. The threshold for the D: disk is 80%.
Per-disk threshold - Maximum percentage of disk growth in %	Specify the maximum percentage of disk growth that can occur on individual disks before an event is raised. Use commas to separate multiple thresholds. For example: `C:=80,D:=120` In this example, the threshold for maximum disk growth on the C: disk is 80%. The threshold for the D: disk is 120%.
Data Collection	
Collect data for available disk space?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of available disk space for the selected drives. The default is unselected.
Collect data for disk utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns utilization details for logical disk space (%), used space (%), threshold (%), total space (MB), free space (MB). The default is unselected.
Collect data for disk growth?	Select Yes to collect data for charts and reports. If enabled, data collection returns the percentage of disk growth from the previous iteration to the current iteration. The default is unselected.

DNSConnectivity

Use this Knowledge Script to check connectivity between a managed computer and its DNS server. This script raises an event if the connection to the DNS server fails.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the connection to the DNS server fails. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the DNS lookup and connection to the DNS server were successful, or • **0** -- the connection is not successful. The default is n.
Remote DNS hostname	Specify the name of the DNS server whose connection should be checked. If you do not enter a hostname, the default DNS server for the managed computer is used. The default is `wns1.HOME.net`.
DNS domain name	Provide the name of the DNS domain for the specified DNS server. Leave blank to use the local domain for the managed computer. The default is `HOME.net`.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the connection to the DNS server fails. The default is 8 (red event indicator).

FailedLogon

Use this Knowledge Script to monitor the number of failed non-interactive logon attempts to the server since the last interval. The result is always zero for the first interval so that the script can establish a baseline for subsequent checks.

For example, this script raises an event if you run this script on a computer and unsuccessfully attempt to log onto that computer using the `net use` command. This script does **not** raise an event for a failed interactive logon attempt, even a failed interactive login attempt from a remote desktop.

Use this script to determine whether password guessing programs are being used on the server. If you use this script to monitor events, the script raises an event for each failed logon attempt. If you choose to collect data, the script reports the total number of logon failures.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the number of failed logon attempts exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of logon failures. The default is n.
Failed logon threshold	Specify the maximum number of failed logon attempts allowed before an event is raised. The default is 0. **Tip** If you are seeing too many insignificant events from users entering passwords incorrectly, determine a "typical" logon failure pattern (for example 5 per 24 hours) and set this parameter accordingly.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of failed logon attempts exceeds the threshold. The default is 5 (red event indicator).

FileChanged

Use this Knowledge Script to determine whether a specified file has changed since the last monitoring interval. This script compares the current size, time stamp, and attributes for a file to the size, time stamp, and attribute settings found for the file the last time the script ran.

You can choose to raise an event if the size, time stamp, or attribute indicates the file has been modified, or raise an event if any of these properties indicates the file has *not* been changed since the last monitoring interval.

Because this script checks the file properties rather than the file content, you can use this script with almost any file type.

Because this script can raise an event if a particular file has changed or when a file you expect to change has not been modified, you can use the script many different ways to monitor your environment.

For example, you might have an application that runs nightly regression tests and generates a report of the results. You can use this script to raise an event when the time stamp for the regression report is not modified, indicating that the test harness might have failed or other problems occurred in producing the expected report. If no event is raised, you can assume that a new report was generated successfully.

In addition, because you can selectively monitor file size, modification time, and attributes, and set severity levels for these properties independently, you can get clearer insight into the changes made to key files and respond accordingly. For example, you can monitor the file modification time for a file and receive a warning or raise an informational event when this property changes. You can raise a critical severity event or receive an e-mail message if a file's attribute changes to read-only or suddenly becomes writable.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Create event if file size changed?	Select **Yes** to raise an event if the file size has changed since the last time the job ran. The default is unselected.
Severity - Size changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the file size has changed. The default is 15 (yellow event indicator).
Create event if file time changed?	Select **Yes** to raise an event if the modification time of the file has changed since the last time the job ran. The default is Yes.
Severity - Time changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the modification time has changed. The default is 15 (yellow event indicator).

Description	How to Set It
Create event if file attribute changed?	Select **Yes** to raise an event if an attribute of the file has changed since the last time the job ran. The default is unselected.
Severity - Attribute changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the file attribute has changed. The default is 15 (yellow event indicator).
Create event if file does not exist?	Select **Yes** to raise an event if the file you want to monitor does not exist. By default, events are not raised.
Severity - File does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the file does not exist. The default is 15 (yellow event indicator).
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the FileChanged job fails unexpectedly. The default is 5 (red event indicator).
Monitoring	
File path	Specify the full path to the file you want to monitor. For example: `C:\Temp\myfile.txt`
Monitor file for...	**...changes**. Select this option to raise events when there are changes to the file. **...NO changes**. Select this option to raise events when there are no changes to the file.

FilesCompare

Use this Knowledge Script to compare the sizes, time stamps, and attributes of two files. You can choose which properties to compare and the event severity if the script finds differences between the specified properties.

Because this script checks the file properties rather than the file content, you can use this script with almost any file type.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if sizes are different?	Set to **y** to raise an event if the file size of File #1 is different from the file size for File #2. The default is y.
Raise event if modification times are different?	Set to **y** to raise an event if the file modification time for File #1 is different from the file modification time for File #2. The default is y.
Raise event if attributes are different?	Set to **y** to raise an event if the file attributes for File #1 are different from the file attributes for File #2. The default is y.
Compare file #1	Provide the full path to the first file to compare. For example: `C:\Temp\myfile.doc`.
Compare file #2	Provide the full path to the second file to compare.
Event severity level for size difference	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a size difference exists. The default is 5 (red event indicator).
Event severity level for time difference	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a time difference exists. The default is 5 (red event indicator).
Event severity level for attribute difference	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an attribute difference exists. The default is 5 (red event indicator).

FileSizeSum

Use this Knowledge Script to monitor the total size of two files. This script raises an event if the total size of the two files exceeds the threshold you set.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Create event if the sum of the size of both files is above the threshold?	Select **Yes** to raise an event if the total size of both files exceeds the threshold you set. The default is Yes.
Severity - Sum size above threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the size of both files exceeds the threshold. The default is 15 (yellow event indicator).
Create event if any file is missing?	Select **Yes** to raise an event if either of the specified files is missing. The default is Yes.
Severity - File missing	Set the event severity level, from 1 to 40, to indicate the importance of an event if either of the specified files is missing. The default is 15 (yellow event indicator).
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the FileSizeSum job fails unexpectedly. The default is 5 (red event indicator).
Data Collection	
Collect file size sum data?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the total size of the two files you specify. The default is unselected.
Monitoring	
Select first file ...	Click **Browse [...]** to select the first of the two files to monitor.
Select second file ...	Click **Browse [...]** to select the second of the two files to monitor.
Sum size threshold	Specify the maximum file size allowed before an event is raised. The default is 2. **Note** Select units for the file size in the *File size scale* parameter.

Description	How to Set It
File size scale	Select the unit of file size. The choices are: • bytes • kilobytes • megabytes • gigabytes • terabytes The default is megabytes.

FilesOpen

Use this Knowledge Script to monitor the number of files currently open through a shared network drive or by a user who logged onto the computer remotely, for example, by using the `net use` command. This script does *not* raise an event if a file is opened by a user who interactively logged onto the computer.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the number of open files exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. The default is n.
Maximum number of files open threshold	Specify the maximum number of files that can be open before an event is raised. The default is 200.
Event severity level for open files	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of open files exceeds the threshold. The default is 5 (red event indicator).
Event severity level for an unexpected Knowledge Script error	Set the event severity level, from 1 to 40, to indicate the importance of an event in which FilesOpen job fails unexpectedly. The default is 35 (magenta event indicator).

FindFiles

Use this Knowledge Script to monitor the number of files that match a set of criteria. This script raises an event if the number of matching files exceeds the threshold you specify. This job fails if the time required to find a file exceeds the schedule interval.

Resource Object

Misc Device folder

Default Schedule

The default schedule for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if threshold is exceeded?	Select **Yes** to raise an event if the number of files found that match your criteria exceeds the threshold you specify. The default is Yes.
Severity -- Exceeded threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of matching files exceeds the threshold. The default is 11 (yellow event indicator).
Raise event if a folder cannot be accessed?	Select **Yes** to raise an event if the folder you specify in the *Root folder to begin the search* parameter does not exist or cannot be accessed because the account under which the NetIQ Client Resource Monitor service (`NetIQmc`) is running does not have permission to open the folder. The default is unselected.
Severity - Folder not accessible	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the specified folder does not exist or cannot be accessed. The default is 25 (blue event indicator).
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the FindFiles job fails unexpectedly. The default is 5 (red event indicator).
Data Collection	
Collect file count data?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of files that match your filtering criteria. The default is unselected.
Monitoring	
Logical drive letter(s) to search	Provide a comma-separated list, with no spaces, of the letters representing the logical drives you want to search. For example: `C,D`.
Root folder to begin the search	Provide the path to the folder on each drive where the search should begin. For example, enter `Documents and Settings\Administrator\My Documents` to begin searching in the `My Documents` folder. The default is `users`.

Description	How to Set It
File name(s), can use * and ? wildcards	Provide the filenames to search for. Use the * wildcard to represent any number of characters. Use the ? wildcard to represent any single character. The default is *.* (all files). You can enter only one filename here, but with the use of wildcards, you can search for multiple files.
Search subfolders?	Select **Yes** to search any subfolders of the root folder in which your search begins. The default is unselected.
File count threshold	Specify the maximum number of files that can be found that match your criteria before an event is raised. The default is 500.
File Filters	
File Attributes Filter	
File attribute operator	Select the operator (AND or OR) to apply to the criteria in the *File Attributes Filter* parameters. For example, instruct the script to search for files that have the *Archive attribute* AND the *Hidden attribute*. The default is OR.
Archive attribute	Select **Yes** to search for files that have the Archive attribute. The default is Yes.
Hidden attribute	Select **Yes** to search for files that have the Hidden attribute. The default is Yes.
Read-only attribute	Select **Yes** to search for files that have the Read-only attribute. The default is Yes.
System attribute	Select **Yes** to search for files that have the System attribute. The default is Yes.
Date Modified Filter	
Apply date modified filter?	Select **Yes** to apply a search filter that considers the date on which a file was modified. The default is unselected.
Select time range	Click **Browse [...]** to open the time browser. Set a specific or sliding date/time range for the date/time on which files were modified. The default is a sliding range of 1 Day with the End now option selected. A specific date/time range defines a specific start and end date and time, for example: `1/1/2004 12:00 AM to 1/31/2004 11:59 PM.` A sliding date/time range defines a time range relative to the start time of the Knowledge Script job. For example, a sliding date/time range of 1 Day extends from 12:00 AM of the previous day to 11:59 PM of the previous day (the entire 24-hour period of the day prior to the day the script runs). The **End now** option for the sliding date/time range extends the time range up to the start time of the Knowledge Script job. For example, if the job runs at 3:00 PM with a sliding range of 1 Day, then the time range covered is 12:00 AM of the previous day to 3:00 PM of the current day.
File Size Filter	
Apply file size filter?	Select **Yes** to apply a search filter that considers the size of a file. The default is unselected.
File size	Set the number of units that define the file size. The type of units are set in the *File size scale* parameter. The default is 2.
File size scale	Set the type of unit that defines the file size (for example, kilobytes). The default is megabytes.
File size operator	Select the operator that defines the file size (for example, less than 2 megabytes). The default is greater than.

FolderFileCount

Use this Knowledge Script to monitor the number of files in a folder that match a set of criteria. This script raises an event if the number of matching files per folder exceeds the threshold you specify.

Resource Object

Misc Device folder

Default Schedule

The default schedule for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if threshold is exceeded?	Select **Yes** to raise an event if the number of files found matching your criteria exceeds the threshold you specify. The default is Yes.
Severity - Exceeded threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of matching files exceeds the threshold. The default is 11 (yellow event indicator).
Raise event if a folder cannot be accessed?	Select **Yes** to raise an event if the folder you specify in the *Root folder to begin the search* parameter does not exist or cannot be accessed because the account under which the NetIQ Client Resource Monitor service (`NetIQmc`) is running does not have permission to open the folder. The default is unselected.
Severity - Folder not accessible	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the specified folder does not exist or cannot be accessed. The default is 25 (blue event indicator).
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the FolderFileCount job fails unexpectedly. The default is 5 (red event indicator).
Data Collection	
Collect file count data?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of folders with a file count that exceeds your threshold and the number of files per folder that match your filtering criteria. The default is unselected.
Monitoring	
Logical drive letter(s) to search	Type a comma-separated list, with no spaces, of the letters representing the logical drives you want to search. For example: `C,D`.
Root folder to begin the search	Type the path to the folder on each drive where you want to begin searching. For example, `Documents and Settings\Administrator\My Documents` to begin searching in the `My Documents` folder. The default is `users`.

Description	How to Set It
File name(s), can use * and ? wildcards	Type the filenames to search for. Use the * wildcard to represent any number of characters; use the ? wildcard to represent any single character. The default is ***.*** (all files). You can enter only one filename here, but with the use of wildcards, you can search for multiple files.
Search subfolders?	Select **Yes** to search any subfolders of the root folder in which your search begins. The default is unselected.
File count threshold per folder	Specify the maximum number of files per folder that can be found that match your criteria before an event is raised. The default is 500.
File Filters	
File Attributes Filter	
File attribute operator	Select the operator (AND or OR) to apply to the criteria in the *File Attributes Filter* parameters. For example, instruct the script to search for files that have the *Archive attribute* AND the *Hidden attribute*. The default is OR.
Archive attribute	Select **Yes** to search for files that have the Archive attribute. The default is unselected.
Hidden attribute	Select **Yes** to search for files that have the Hidden attribute. The default is unselected.
Read-only attribute	Select **Yes** to search for files that have the Read-only attribute. The default is unselected.
System attribute	Select **Yes** to search for files that have the System attribute. The default is unselected.
Date Modified Filter	
Apply date modified filter?	Select **Yes** to apply a search filter that considers the date on which a file was modified. The default is unselected.
Select time range	Click **Browse [...]** to set a specific or sliding date/time range for the date/time on which files were modified. The default is a sliding range of 1 Day with the End now option selected. A specific date/time range defines a specific start and end date and time, for example: 1/1/2004 12:00 AM to 1/31/2004 11:59 PM. A sliding date/time range defines a time range relative to the start time of the Knowledge Script job. For example, a sliding date/time range of 1 Day extends from 12:00 AM of the previous day to 11:59 PM of the previous day (the entire 24-hour period of the day prior to the day the script runs). The **End now** option for the sliding date/time range extends the time range up to the start time of the Knowledge Script job. For example, if the job runs at 3:00 PM with a sliding range of 1 Day, then the time range covered is 12:00 AM of the previous day to 3:00 PM of the current day.
File Size Filter	
Apply file size filter?	Select **Yes** to apply a search filter that considers the size of a file. The default is unselected.
File size	Specify the number of units that define the file size. The type of units are set in the *File size scale* parameter. The default is 10.
File size scale	Specify the type of unit that defines the file size (for example, kilobytes). The default is megabytes.
File size operator	Specify the operator that defines the file size (for example, less than 10 megabytes). The default is greater than.

FolderSize

Use this Knowledge Script to monitor the size of folders containing files that match a set of criteria. For example, you can monitor for folders over 100 MB that contain `MPG` or `JPG` files, and you can further refine your criteria to only include `MPG` or `JPG` files over a particular size. This script raises an event if the size of any folder exceeds the threshold you specify.

Resource Object

Misc Device folder

Default Schedule

The default schedule for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if threshold is exceeded?	Select **Yes** to raise an event if the size of a folder containing files matching your criteria exceeds the threshold you specify. The default is Yes.
Severity - Exceeded threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the folder size exceeds the threshold. The default is 11 (yellow event indicator).
Raise event if a folder cannot be accessed?	Select **Yes** to raise an event if the folder you specify in the *Root folder to begin the search* parameter does not exist or cannot be accessed because the account under which the NetIQ Client Resource Monitor service (`NetIQmc`) is running does not have permission to open the folder. The default is unselected.
Severity - Folder not accessible	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the specified folder does not exist or cannot be accessed. The default is 25 (blue event indicator).
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the FolderSize job fails. The default is 5 (red event indicator).
Data Collection	
Collect folder count data?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of folders whose file size exceeds the threshold. The default is unselected.
Monitoring	
Logical drive letter(s) to search	Type a comma-separated list, with no spaces, of the letters representing the logical drives you want to search. For example: `C,D`.
Root folder to begin the search	Type the path to the folder on each drive in which you want to begin searching. For example, enter `Documents and Settings\Administrator\My Documents` to begin searching in the `My Documents` folder. The default is `users`.

Description	How to Set It
File name(s), can use * and ? wildcards	Type the filenames to search for. Use the * wildcard to represent any number of characters; use the ? wildcard to represent any single character. The default is *.* (all files). You can enter only one filename here, but with the use of wildcards, you can search for multiple files.
Search subfolders?	Select **Yes** to search any subfolders of the root folder in which your search begins. The default is Yes.
Folder size threshold	Specify the number of units that define the folder size. The type of units is set in the *Folder size scale* parameter. The default is 10.
Folder size scale	Specify the type of unit that defines the folder size (for example, kilobytes). The default is megabytes.
Folder size operator	Specify the operator that defines the folder size (for example, less than 10 megabytes). The default is greater than.
File Filters	
File Attributes Filter	
File attribute operator	Select the operator (AND or OR) to apply to the criteria in the *File Attributes Filter* parameters. For example, instruct the script to search for files that have the *Archive attribute* AND the *Hidden attribute*. The default is OR.
Archive attribute	Select **Yes** to search for files that have the Archive attribute. The default is unselected.
Hidden attribute	Select **Yes** to search for files that have the Hidden attribute. The default is unselected.
Read-only attribute	Select **Yes** to search for files that have the Read-only attribute. The default is unselected.
System attribute	Select **Yes** to search for files that have the System attribute. The default is unselected.
Date Modified Filter	
Apply date modified filter?	Select **Yes** to apply a search filter that considers the date on which a file was modified. The default is unselected.
Select time range	Click **Browse [...]** to set a specific or sliding date/time range for the date on which files were modified. The default is a sliding range of 1 Day with the End now option selected. A specific date/time range defines a specific start and end date and time, for example: `1/1/2004 12:00 AM to 1/31/2004 11:59 PM.` A sliding date/time range defines a time range relative to the start time of the Knowledge Script job. For example, a sliding date/time range of 1 Day extends from 12:00 AM of the previous day to 11:59 PM of the previous day (the entire 24-hour period of the day prior to the day the script runs). The **End now** option for the sliding date/time range extends the time range up to the start time of the Knowledge Script job. For example, if the job runs at 3:00 PM with a sliding range of 1 Day, then the time range covered is 12:00 AM of the previous day to 3:00 PM of the current day.
File Size Filter	
Apply file size filter?	Select **Yes** to apply a search filter that considers the size of a file. The default is unselected.
File size	Specify the number of units that define the file size. The type of units are set in the *File size scale* parameter. The default is 5.

Description	How to Set It
File size scale	Specify the type of unit that defines the file size (for example, kilobytes). The default is megabytes.
File size operator	Specify the operator that defines the file size (for example, less than 5 megabytes). The default is greater than.

IntervalCounter

Use this Knowledge Script to monitor changes in any performance monitor counter. You can specify a consecutive number of times that the *Counter delta value threshold* parameter must be exceeded before the script raises an event. This script automatically raises an event if it does not find the counter to monitor.

This script collects the counter value delta between script executions for the object\counter\instance you are monitoring. A negative counter value delta indicates that the counter value has decreased.

Prerequisites

If the Operator Console or Control Center is installed on Windows Server 2003, the Remote Registry service on the console computer must be running. If the Remote Registry service is down when you attempt to configure this script, the console displays an error message indicating AppManager was unable to connect to the remote computer.

If the Operator Console or Control Center is installed on Windows Vista, the Remote Registry service on the console computer must be running. If the Remote Registry service is down when you attempt to configure this script, the console becomes unresponsive.

Resource Objects

Any discovered Windows computer or application server, such as Exchange Server, SQL Server, or Proxy Server

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Set to **y** to collect data for charts and reports. When enabled, data collection returns the counter value delta between script executions for the object, counter, or instance you are monitoring. The default is n.
Event when over threshold?	Set to **y** to raise an event if the counter value exceeds the threshold. The default is y.
Counter delta value threshold	Specify the maximum allowed value for the difference between the counter value from the previous job iteration and the current job iteration. The default is 600.
Counter to monitor	Enter the object, counter, or instance name, or click **Browse [...]** to select the object, counter, and instances to monitor. The default is `Objects\Threads\`. **Note** You can also start the System Monitor and click **Add [+]** in the toolbar. Use the format: `<object>\<counter>\<instance>\`. You can enter multiple instances, separated by commas. For example: `Process\% Privileged Time\mapisp32,mqsvc`. If the counter does not have an instance name, end the string with a backslash: `Process\% Privileged Time\`. If an instance is a parent of multiple instances (for example, if you have a logical disk 0 with partitions C: and D:), enter the complete instance name exactly as displayed in the Performance Monitor (for example, `"0 ==> C:"`).

Description	How to Set It
Consecutive times	Specify the maximum number of consecutive times the counter must exceed the threshold before this script raises an event. The default is 1.
Event severity level - Over threshold	Set the event severity level, from 1 to 40 to indicate the importance of an event in which the counter value exceeds threshold. The default is 8 (red event indicator).
Event severity level...	Set the event severity level, from 1 to 40 to indicate the importance of an event in which the monitored counter or instance cannot be found. The default is 15 (yellow event indicator).

LogicalDiskStats

Use this Knowledge Script to monitor logical disk I/O and busy statistics gathered from performance counter values in Performance Monitor:

- Disk transfers per second
- Disk reads per second
- Disk writes per second
- Disk operation time in milliseconds
- Disk queue length

This script raises an event if a monitored value exceeds the threshold you specify.

Each time it runs, this script automatically monitors all logical disks on a server and all shared drives in a cluster. When this script runs on a cluster virtual server object, it monitors statistics for all shared drives that are active at the time. When this script runs on a physical Windows server, it monitors statistics for those drives that are not shared as part of a cluster, such as local fixed drives and removable drives.

You can choose to exclude any drive from monitoring or to monitor mount points configured on logical drives. Mount points must be configured as described in the following Microsoft Knowledge Base article: http://support.microsoft.com/kb/280297. Performance counter values are not created for mount points configured incorrectly. Therefore, this script raises an event when mounts points are not configured correctly, indicating an error when reading the disk.

This script ignores CDROMs, floppy drives, or other removable media whose size cannot be determined.

Resource Object

Logical disk object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the LogicalDiskStats job fails. The default is 15.
Logical Disk I/O	
Raise event if disk transfers exceed threshold?	Select **Yes** to raise an event if the number disk transfers per second exceeds the threshold you set. The default is Yes.
Event severity when disk transfers exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event in which the number of times data is transferred on a disk exceeds the threshold you set. The default is 8.
Threshold - Maximum disk transfers per second	Specify the maximum number of disk transfers that can occur per second before an event is raised. The default is 80.

Parameter	How to Set It
Raise event if disk reads exceed threshold?	Select **Yes** to raise an event if the number of disk reads per second exceeds the threshold you set. The default is Yes.
Event severity when disk reads exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event in which the number of times data is read from a disk exceeds the threshold you set. The default is 8.
Threshold - Maximum disk reads per second	Specify the maximum number of disk reads that can occur per second before an event is raised. The default is 50.
Raise event if disk writes exceed threshold?	Select **Yes** to raise an event if the number of disk writes per second exceeds the threshold you set. The default is Yes.
Event severity when disk writes exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event in which the number of times data is written to a disk exceeds the threshold you set. The default is 8.
Threshold - Maximum disk writes per second	Specify the maximum number of disk writes that can occur per second before an event is raised. The default is 50.
Logical Disk Busy	
Raise event if disk operation time exceeds threshold?	Select **Yes** to raise an event if the length of time per disk operation exceeds the threshold you set. The default is Yes.
Event severity when disk operation time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the length of time it takes for a disk operation to complete exceeds the threshold you set. The default is 5.
Threshold - Maximum disk operation time	Specify the maximum length of time that a disk operation can take to complete before an event is raised. The default is 100 milliseconds.
Raise event if disk queue length exceeds threshold?	Select **Yes** to raise an event if the number of requests in the disk queue exceeds the threshold you set. The default is Yes.
Event severity when disk queue length exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of requests in the disk queue exceeds the threshold you set. The default is 5
Threshold - Maximum disk queue length	Specify the maximum number of requests that can be in queue before an event is raised. The default is 1 request.
Monitoring	
Drives to exclude	Provide a comma-separated list of the drives you do not want to monitor. This script automatically monitors all drives except those listed in this parameter. The asterisk (*) is an acceptable wildcard. For example, to exclude the C: drive and disks or mount points that begin with `\crate`, specify the following: `c:,e:\crate*` The * wildcard is valid only at the end of an expression, not in the middle or beginning of an expression.
Monitor mount points?	Select **Yes** to allow the script to monitor mount points (mapped drives). The default is Yes.
Data Collection	
Logical Disk I/O	
Collect data for disk transfers per second?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of disk transfers per second for the monitoring period. The default is unselected.

Parameter	How to Set It
Collect data for disk reads per second?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of disk reads per second for the monitoring period. The default is unselected.
Collect data for disk writes per second?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of disk writes per second for the monitoring period. The default is unselected.
Logical Disk Busy	
Collect data for disk operation time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the length of disk operations, in milliseconds, for the monitoring period. The default is unselected.
Collect data for disk queue length?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of requests in queue for the monitoring period. The default is unselected.

MemByProcess

Use this Knowledge Script to monitor process memory usage. This script monitors individual memory use for each specified process, and the total memory use for all specified processes. If a process is not found, this script assumes that the process is not currently running, and reports 0 as the memory result.

You can use this script to monitor multiple processes with the same name, such as the process spawned by each instance of `svchost.exe` running on the same computer.

Notes

- This script does not detect invalid process names. If you type an invalid process name, the script assumes that the process is not running, and reports 0 as the result.
- This script raises an event if the memory usage for a named process exceeds the threshold, with one exception: the Windows System Idle process. The System Idle process indicates the percentage of idle CPU resources. If no applications are running, this process indicates a high idle capacity. The high percentage exceeds the threshold and raises an event indicating that the System Idle Process consumes high CPU resources. You can safely ignore this event message because the high percentage refers to the high idle capacity and not high CPU usage.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Create event for each process that exceeds the threshold?	Select **Yes** to raise an event if the memory for an individual process exceeds the threshold you specify. The default is Yes.
Severity - Individual process memory high	Set the event severity level, from 1 to 40, to indicate the importance of an event in which individual process memory usage exceeds the threshold. The default is 8 (red event indicator).
Create event if the sum of all processes exceeds the threshold?	Select **Yes** to raise an event if the memory usage for all processes exceeds the threshold you specify. The default is Yes.
Severity -- Total process memory high	Set the event severity level, from 1 to 40, to indicate the importance of an event in which total process memory usage exceeds the threshold. The default is 15 (yellow event indicator).
Severity -- Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MemByProcess job fails unexpectedly. The default is 5 (red event indicator).

Description	How to Set It
Data Collection	
Collect data for each process?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns data for individual processes you are monitoring, including process name, memory utilization, and the memory utilization threshold you specified. The default is unselected. **Note** If a process is not found, the script assumes that the process is not currently running, and reports 0 as the memory result.
Collect data for all processes?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns data for all processes you are monitoring, including the process count, total memory utilization, and the memory utilization threshold you specified. The default is unselected. **Note** If a process is not found, the script assumes that the process is not currently running, and reports 0 as the memory result.
Monitoring	
Processes	Provide one or more process names, separated by commas (,) and no spaces. The default is `explorer,lsass`. **Note** Under circumstances where multiple instances of a process are running on a computer (for example, `svchost`), Windows adds a number to each successive instance of the process beginning with the second instance (for example, `svchost`, `svchost#1`, `svchost#2`). You can monitor each process instance by entering the process name, including the added number. **To see a list of distinct process names:** 1. From the Control Panel, double-click **Administrative Tools** and then double-click **Performance**. 2. Click **Add** (+). 3. From the Performance object list, select **Process**. 4. Click **Select instances from list** and then scroll to find the process names. 5. Click **Add**. **Note** The value of the *Processes* parameter must be an exact match (including case-sensitivity) of the process name in the Performance Object field of PerfMon.
Maximum threshold for memory for each process	Specify the maximum amount of memory each process can use before an event is raised. The default is 20000. Use the *Memory scale* parameter to define the threshold scale.
Maximum threshold for memory for all processes	Specify the maximum amount of memory all processes can use before an event is raised. The default is 32000. Use the *Memory scale* parameter to define the threshold scale.
Memory scale	Select the scale for the memory threshold you specify: bytes, kilobytes, megabytes, gigabytes, terabytes. The default is kilobytes.

MemUtil

Use this Knowledge Script to monitor usage of physical memory, virtual memory, and paging files. This script raises an event if the usage of a monitored item exceeds the threshold. In addition, this script generates data streams for all monitored items.

Resource Objects

Physical memory object

Virtual memory object

Paging files folder

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MemUtil job fails. The default is 5.
Raise event if physical memory usage exceeds threshold?	Select **Yes** to raise an event if physical memory usage exceeds the threshold you set. The default is Yes.
Event severity when physical memory usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which physical memory usage exceeds the threshold you set. The default is 5.
Raise event if virtual memory usage exceeds threshold?	Select **Yes** to raise an event if virtual memory usage exceeds the threshold you set. The default is Yes.
Event severity when virtual memory usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which virtual memory exceeds the threshold you set. The default is 5.
Raise event if paging file usage exceeds threshold?	Select **Yes** to raise an event if paging file usage exceeds the threshold you set. The default is Yes.
Event severity when paging file usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which paging file usage exceeds the threshold. The default is 5.
Monitoring	
Use virtual machine performance counters if available?	Select **Yes** to monitor VMware performance counter data on virtual machines, if available, instead of physical host counters. The default is Yes. VMware performance counters do not provide virtual memory or paging file data. If you select Yes, only physical memory usage data is monitored.
Thresholds	

Description	How to Set It
Threshold - Maximum physical memory usage	Specify the maximum percentage of physical memory that can be in use before an event is raised. The default is 90%.
Threshold - Maximum virtual memory usage	Specify the maximum percentage of virtual memory that can be in use before an event is raised. The default is 90%.
Threshold - Maximum paging file usage	Specify the maximum percentage of the paging file that can be in use before an event is raised. The default is 70%.
Data Collection	
Collect data for physical memory usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of physical memory usage during the monitoring period. The default is unselected.
Collect data for virtual memory usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of virtual memory usage during the monitoring period. The default is unselected.
Collect data for paging file usage?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the size of the paging file during the monitoring period. The default is unselected.

NetSession

Use this Knowledge Script to list the network sessions connected to a computer. This script raises an event if the number of sessions exceeds the threshold you specify. In addition, this script generates data streams for the number of connected sessions.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the number of sessions exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. The default is n.
Maximum connected sessions threshold	Specify the maximum number of sessions that can be connected at one time before an event is raised. The default is 100.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of sessions exceeds the threshold. The default is 8 (red event indicator).

NetworkBusy

Use this Knowledge Script to monitor the traffic on network interface cards (NICs). This script raises an event if the network interface's bandwidth utilization exceeds the threshold you specify. This script skips interface card number 1 as a loopback.

Note
This script uses the Network Interface Performance Monitor counter to perform its monitoring task. If this performance counter is not available, install the SNMP services to make the counter available.

Resource Objects

Non-WAN wrapper network interface cards

Network interface folder

Default Schedule

The default schedule for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the network interface's bandwidth utilization exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the percentage of network bandwidth in use. The default is n.
Maximum percentage network utilization threshold	Specify the maximum percentage of network bandwidth that can be in use before an event is raised. The default is 35%.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which bandwidth utilization exceeds the threshold. The default is 5 (red event indicator).

PagingHigh

Use this Knowledge Script to monitor reads and writes per second to the pagefile. This script raises an event if the number of reads and writes per second exceeds the threshold you specify. In addition, this script generates data streams for the number of read and writes per second.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the number of reads and writes exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. When enabled, data collection returns the number of reads and writes per second during the monitoring interval. The default is n.
Maximum pagefile activity per second threshold	Specify the maximum number of reads and writes to the pagefile allowed per second before an event is raised. The default is 200.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of reads and writes per second exceeds the threshold. The default is 5 (red event indicator).

PhysicalDiskStats

Use this Knowledge Script to monitor physical disk I/O and busy values:

- Disk transfers per second
- Disk reads per second
- Disk writes per second
- Disk operation time in milliseconds
- Disk queue length

This script raises an event if a monitored value exceeds the threshold you specify.

Resource Objects

Physical disk object

Default Schedule

By default, this script runs every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Physical Disk I/O Notification	
Raise event if disk transfers exceed threshold	Select **Yes** to raise an event if the number disk transfers per second exceeds the threshold you set. The default is Yes.
Event severity when disk transfers exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event in which the number of times data is transferred on a disk exceeds the threshold you set. The default is 8.
Raise event if disk reads exceed threshold?	Select **Yes** to raise an event if the number of disk reads per second exceeds the threshold you set. The default is Yes.
Event severity when disk reads exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event in which the number of times data is read from a disk exceeds the threshold you set. The default is 8.
Raise event if disk writes exceed threshold?	Select **Yes** to raise an event if the number of disk writes per second exceeds the threshold you set. The default is Yes.
Event severity when disk writes exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event in which the number of times data is written to a disk exceeds the threshold you set. The default is 8.
Physical Disk Busy Notification	
Raise event if disk operation time exceeds threshold?	Select **Yes** to raise an event if the length of time per disk operation exceeds the threshold you set. The default is Yes.
Event severity when disk operation time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the length of time it takes for a disk operation to complete exceeds the threshold you set. The default is 5.

Parameter	How to Set It
Raise event if disk queue length exceeds threshold?	Select **Yes** to raise an event if the number of requests in the disk queue exceeds the threshold you set. The default is Yes.
Event severity when disk queue length exceeds threshold	Set the event severity, from 1 to 40, to indicate the importance of an event in which the number of requests in the disk queue exceeds the threshold you set. The default is 5
Raise event if job fails?	Select **Yes** to raise an event if the PhysicalDiskStats job fails. The default is Yes.
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the PhysicalDiskStats job fails. The default is 15.
Data Collection	
Physical Disk I/O Data Collection	
Collect data for disk transfers per second?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of disk transfers per second for the monitoring period. The default is unselected.
Collect data for disk reads per seconds?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of disk reads per second for the monitoring period. The default is unselected.
Collect data for disk writes per second?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of disk writes per second for the monitoring period. The default is unselected.
Physical Disk Busy Data Collection	
Collect data for disk operation time?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the length of disk operations, in milliseconds, for the monitoring period. The default is unselected.
Collect data for disk queue length?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of requests in queue for the monitoring period. The default is unselected.
Monitoring	
Physical Disk I/O Monitoring	
Threshold - Maximum disk transfers per second	Specify the maximum number of disk transfers that can occur per second before an event is raised. The default is 80.
Threshold - Maximum disk reads per second	Specify the maximum number of disk reads that can occur per second before an event is raised. The default is 50.
Threshold - Maximum disk writes per second	Specify the maximum number of disk writes that can occur per second before an event is raised. The default is 50.
Physical Disk Busy Monitoring	
Threshold - Maximum disk operation time	Specify the maximum length of time that a disk operation can take to complete before an event is raised. The default is 100 milliseconds.
Threshold - Maximum disk queue length	Specify the maximum number of requests that can be in queue before an event is raised. The default is 1 request.

PortHealth

Use this Knowledge Script to check whether system ports are working properly. This script raises an event if a port is not operating. In addition, this script generates data streams for port availability.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if a port is not operating. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • 100 -- the port is operating properly • 0 -- the port is not operating The default is n.
Network addresses	Provide the network addresses for which you want to check port availability. Separate the addresses with commas (,) and no spaces. Use the format: `<host_ID>:<port_number>`. The host ID can be a hostname or IP address. For example: `www.storm.com:8008,1.10.10.10:30`. The default is `www.netiq.com:80`.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a port is not operating. The default is 8 (red event indicator).

PrinterHealth

Use this Knowledge Script to monitor the health of printers. This script checks whether any specified printer is paused or if the printer queue length exceeds the threshold you specify, and raises an event if either condition exists. This script also raises an event if it finds general printing errors such as a printer that is out of paper or jammed.

You can set this script to discover printers dynamically each time it runs. If you discover printers dynamically, printers that were not discovered when you ran Discovery_NT are not reflected in the TreeView pane.

Note
To run this script successfully, avoid using special characters such as, /, -, and # when defining the printer name on the monitored computers. Also, if you run the Discovery_NT Knowledge Script and then delete a local or network printer, run Discovery_NT again.

Resource Objects

Printer folder, if dynamically enumerating printers. If you are not enumerating printers dynamically, you can run this script on the Printer folder or individual printer objects. You can run this script only on a local printer.

Default Schedule

The default schedule for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if a specified printer is paused, if the printer queue length exceeds the threshold you specify, or if the script finds general printing errors. The default is y. This script displays the following event messages when it detects a general printer error: Door Open, Paper Jam, Offline, No Paper, Toner Low, or Service Request.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of print jobs at each interval. The default is n.
Dynamically enumerate at each interval?	Set to **y** to dynamically observe connected printers at each monitoring interval. The default is y.
Maximum printer queue length threshold	Specify the maximum number of print jobs that can be waiting in the queue before an event is raised. The default is 10.
Maximum print job size threshold	Specify the maximum print job size allowed before an event is raised. The default is 200 KB.
Event severity level for printer paused	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the printer is not responding and no jobs are being processed. The printer is off-line, or out of paper or toner, for example. The default is 3 (red event indicator).
Event severity level for printer busy	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of jobs in the printer queue exceeds the threshold. The default is 5 (red event indicator).

Description	How to Set It
Event severity level for job size threshold crossed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the size of the print job exceeds the threshold. The default is 1 (red event indicator).

PrinterQueue

Use this Knowledge Script to monitor a printer's queue length. This script checks the number of queued print jobs for a specified printer. You need to specify the name of the computer that serves the printer and the printer's share name. This script raises an event if the number of queued jobs exceeds the threshold you specify. In addition, this script generates data streams for queue length.

Notes

- Before running this script, ensure the AppManager agent service, `NetIQmc`, is set to run as a domain user account user in the same domain as, or a domain trusted by, the target computer. Use the **Services** Control Panel to identify an account for the service to run as.
- To run this Knowledge Script successfully, *avoid* using special characters such as, /, -, and # when defining the printer name on the monitored computers. Also, if you run the Discovery_NT Knowledge Script and *then* delete a local or network printer, run Discovery_NT again.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Note

This script is not supported on 64-bit systems.

Default Schedule

The default schedule for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the number of queued jobs exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of queued print jobs at each interval. The default is n.
Print server's hostname	Provide the name of the computer that serves the printer you want to monitor.
Server's share name for printer	Provide the name of the share used by the printer server for the printer you want to monitor.
Maximum print queue threshold	Specify the maximum number of print jobs that can be waiting in the queue before an event is raised. The default is 10.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of queued jobs exceeds the threshold. The default is 8 (red event indicator).

ProcessDown

Use this Knowledge Script to determine whether specified processes are running. This script raises an event if a specified process is not running. In addition, this script generates a data stream for process availability.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the process you selected for monitoring is not running. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns data for each named process, either: • **100** -- the process is running; or • **0** -- the process is not running. The default is n.
Processes	Provide one or more process names, separated by commas (,) and no spaces. Do not specify the file extension of the process. For example: `clock,tcpsvcs` **Tip** To monitor processes, AppManager retrieves the name of the performance counter instance associated with the process. If a PID (process identifier) is appended to the counter instance name, you do not need to indicate the PID in this parameter. Use an asterisk (*) instead. For example: • Use an asterisk (*) after the process name to monitor all processes that begin with the string you provide. For example: `clock,tcpsvcs*` • Use an asterisk (*) before the process name to monitor all processes that end with the string you provide. For example: `clock,*tcpsvcs`
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a selected process is not running. The default is 8 (red event indicator).

Processes

Use this Knowledge Script to monitor the number of active processes. This script raises an event if the number of active processes exceeds the threshold you specify. In addition, this script generates data streams for active processes.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the number of active processes exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. The default is n.
Maximum total processes threshold	Specify the maximum number of active processes allowed before an event is raised. The default is 80.
Number of top processes to be displayed	Specify the number of top processes to display in the detail event or data message. Type 0 to display all processes. The default is 10.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active processes exceeds the threshold. The default is 5 (red event indicator).

ProcessUp

Use this Knowledge Script to check whether a specified process is running. This script raises an event if the specified process is running, and can automatically terminate the process if you choose. In addition, this script generates data streams for process status.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Create event if process is found running?	Select **Yes** to raise an event if one or more of the processes you specified in the *Processes* parameter are running. The default is Yes.
Severity - Process running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a specified process is running. The default is 10 (red event indicator).
Create event if process is not running?	Select **Yes** to raise an event if a process you specified in the *Processes* parameter is not running. The default is unselected.
Severity - Process not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a specified process is not running. The default is 10 (red event indicator).
Create event if process is successfully terminated?	Select **Yes** to raise an event a process you specified in the *Processes* parameter is successfully terminated. The default is Yes. **Note** If you set this parameter to **Yes**, also set the *Kill the running process?* parameter to **Yes**.
Severity -- Process successfully terminated	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a process is successfully stopped. The default is 25 (blue event indicator).
Create event if process cannot be terminated?	Select **Yes** to raise an event if a process you specified in *Processes* cannot be terminated. By default, events are enabled. **Note** If you set this parameter to **Yes**, also set the *Kill the running process?* parameter to **Yes**.
Severity -- Failed to kill process	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a specified process cannot be terminated. The default is 10 (red event indicator).
Severity -- Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ProcessUp job fails unexpectedly. The default is 5 (red event indicator).
Data Collection	

Description	How to Set It
Collect data for process status?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns: • **100** -- the specified process is running, or • **0** -- the process is not running. The default is unselected.
Monitoring	
Processes	Provide one or more process names, separated by commas (,) and no spaces. Specify a process name without an extension and use the following format for multiple instances of a process: `iexplore (first instance),iexplore#1 (second instance),iexplore#2 (third instance)`
Kill the running process?	Select **Yes** to automatically stop a specified process. If there are multiple instances of a specified process, all instances are stopped. The default is Yes.

RegistryChange

Use this Knowledge Script to monitor changes in the registry information on 32-bit and 64-bit Windows systems. This script raises an event if a key or value is added, deleted, or changed in the registry. In addition, this script generates data streams for registry changes.

From a specified path, this script searches the registry for changes to registry keys and sub-keys. This information can be valuable in helping you understand the behavior and configuration of the computers you are monitoring, but it can also be expensive in terms of processing time. Because each registry level can contain many sub-keys to check, this script can require a significant period of time to run if you check two or three levels deep in the registry tree.

On 64-bit Windows systems, this script can be configured to monitor registry information for 32-bit or 64-bit programs. For example, to monitor changes to:

- The key that specifies what programs should be run at startup, set the value of the *Monitor 32-bit program registry keys on a 64-bit system?* parameter to **n**, and specify the following registry key:

  `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

- Keys associated with a 32-bit application such as AppManager, set the value of the *Monitor 32-bit program registry keys on a 64-bit system?* parameter to **y**, and specify the registry exactly as it would be specified on a 32-bit system. For example:

  `HKEY_LOCAL_MACHINE\Software\NetIQ\AppManager\4.0`

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 30 minutes**.

If you set this script to check sub-key levels, adjust the schedule. For example, if you are checking two or three sub-levels deep, set this script to run once a day during off-peak hours.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if a key or value is added, deleted, or changed in the registry. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of changes to the registry since the last time the job ran. The detail message includes specific information about each change. The default is n.
Monitor 32-bit program registry keys on a 64-bit system?	On a 64-bit Windows system, set this parameter to **y** to monitor registry information for 32-bit programs. The default value, n, enables you to monitor registry information for 64-bit programs. On a 32-bit Windows system, this parameter is not applicable and will be ignored. **Tip** To monitor registry information for 32-bit programs and 64-bit programs, configure separate Knowledge Script jobs.

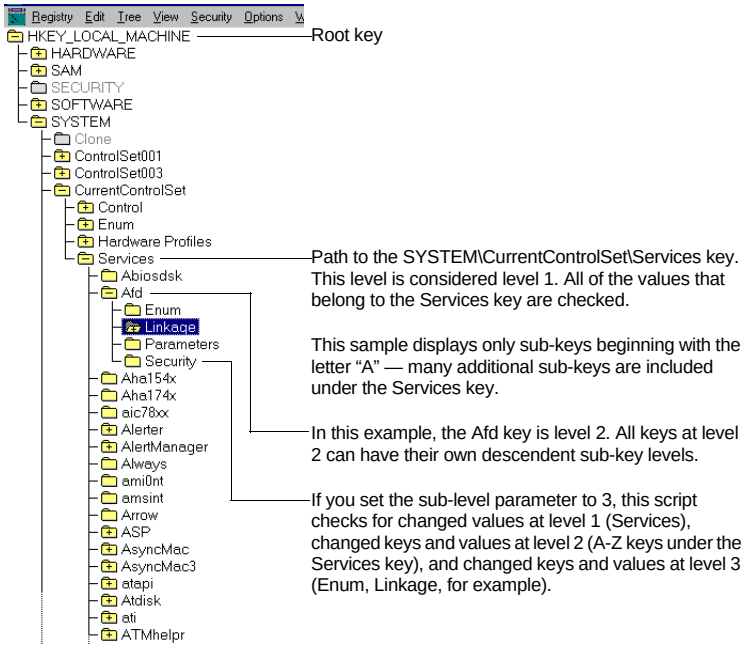
Description	How to Set It
Root key	Type the registry root. Valid root options are: • HKEY_LOCAL_MACHINE • HKEY_CLASSES_ROOT • HKEY_CURRENT_USER • HKEY_USERS The default is HKEY_LOCAL_MACHINE.
Path name	Specify the path to the registry keys to monitor. The default path is SYSTEM\CurrentControlSet\Services. To specify the path to registry information for a 32-bit or 64-bit program, specify a path under HKEY_LOCAL_MACHINE\Software. Although the registry keys for 32-bit programs on a 64-bit system are stored under the HKEY_LOCAL_MACHINE\Software\Wow6432Node key, do **not** specify the Wow6432Node component of the path. Instead, specify the path without the Wow6432Node component, and set the value of the *Monitor 32-bit program registry keys on a 64-bit system?* parameter to **y**. **Note** Use a specific path to the key you want to monitor. Any key can have many sub-levels, and the level specified by this path is always considered level 1.
Sub-level	Specify the number of descendent key levels to monitor, counting the path itself as level 1. The maximum number of key sub-levels you can monitor is 3. The default is 2.
Exceptions	Specify any sub-keys to exclude from monitoring. Exceptions are case-sensitive. Separate sub-keys using commas (,) and no spaces. For example, to exclude CmdLine and SetupType under the Setup sub-key, type: SYSTEM\Setup\CmdLine,SYSTEM\Setup\SetupType.
Event severity level for registry change	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a change in the registry occurs. The default is 8 (red event indicator).
Event severity level for an unexpected Knowledge Script error	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the RegistryChange job fails. The default is 35 (magenta event indicator).

Example of How this Script Is Used

This script traverses the registry to check for changes to registry keys and sub-keys. This information can be extremely valuable in understanding the behavior and configuration of the computers you are monitoring but it can also be expensive in terms of processing time. To understand the impact of running this script, consider the following registry example.

If you set the *Path name* parameter to SYSTEM\CurrentControlSet\Services, the key becomes the first level of monitoring (sub-level 1) and all the keys at that level are checked for changes. If you set the *Sub-level* parameter to 3 for this job, the script then monitors all the values for all the sub-keys under the SYSTEM\CurrentControlSet\Services key and all the values for the sub-keys under the SYSTEM\CurrentControlSet\Services sub-key folders. With these settings, you can monitor a large number of key values but might put undue strain on your system.

As you can see in the following example, each sub-key level you monitor can contain many sub-keys and sub-key values:



One way to control the number of key values you monitor is by choosing the base path carefully. For example, you can set the `Path name` to a specific sub-key such as `SYSTEM\CurrentControlSet\Services\EventLog`. Depending on the number of sub-keys under the base path, however, you might also need to consider how best to set the sub-level parameter.

For example, if you set the *Path name* to `SYSTEM\CurrentControlSet\Services\EventLog` and the *Sub-level* parameter to `3`, the `EventLog` key becomes sub-level 1 and is checked for changes to values. The `EventLog` key contains the `Application`, `Security`, and `System` sub-keys, which as sub-level 2, are checked for new keys and values. Each of these sub-level 2 keys branches further, yielding dozens more keys at sub-level 3, each with values to check.

Because the number of monitored values can expand quickly, it is important to consider either narrowing the key path and sub-levels to check or lengthening the monitoring interval for this script to run effectively.

RemoteServiceDown

Use this Knowledge Script to monitor services on remote computers. You can specify the computers to monitor either directly using the *Machine list* parameter, or in a file containing a list of computer names or addresses.

This script tries to communicate with each of the remote computers in the *Machine list* parameter. This script raises an event if a named service is down or a specified computer cannot be reached from the computer where this script is running.

This script displays event information even if the remote computer is in maintenance mode.

Note
The AppManager agent does not need to be installed on the remote computer you want to monitor, nor does the remote computer need to exist in the TreeView pane of the Operator Console.

When configuring an action for the RemoteServiceDown script, configure the Location to run on the MS (management server) or on a Proxy (a particular managed client computer).

If you instead configure an action to run on the managed client (MC), when a remotely monitored computer is placed into maintenance mode or scheduled maintenance mode, AppManager ignores any event conditions detected on the remote computer but does not disable the action.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if a specified service is down or if a specified computer cannot be reached from the computer where this script is running. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns data for each named service, either: • **100** -- the service is running; or • **0** -- the service is not running. The default is n.
Collect data only on down?	Set to **y** to collect data for charts and reports only when named services are down. If enabled, data collection returns a value of 0 when a service is down. Enable this parameter only if the *Collect data?* parameter is enabled. The default is n.
Machine list	Specify the names of the computers to be monitored. Separate multiple names with commas (,) and no spaces. For example: `AppSrvr,Storm,CorpSrvr`.

Description	How to Set It

File name for machine list	Provide the full path to the file containing the list of computers to test. The file should contain the hostname or IP address for each computer in one or more lines. Each line can have multiple computer names, separated by commas and no spaces. For example:
	`NYC01,NYC02`
	`SALES01,10.15.221.5,SFO01`
	`LABMACH,QATEST`
	The job supports a maximum file size of 32KB. If the file size exceeds 32KB, the job stops and raises an error event message: `Out of string space`.

Services	Provide the names of the services to be monitored. Separate multiple names with commas (,) and no spaces. The default is the NetIQ AppManager Agent service: `NetIQmc`.
Auto-start service?	Set to **y** to automatically restart down services. The default is y.
Event severity level for service down; auto-start failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and auto-start failed. The default is 5 (red event indicator).
Event severity level for service down; auto-start succeeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and auto-start succeeded. The default is 25 (blue event indicator).
Event severity level for service down; don't auto-start	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and you have selected not to restart it. The default is 18 (yellow event indicator).
Event severity level for service not found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a selected service cannot be found. The default is 8 (red event indicator).

RemoteServiceDownLR

Use this Knowledge Script to monitor services on remote computers. You specify the computers and services to monitor. A service that is detected as down can be restarted. The Windows services include those that are not discovered by AppManager for Microsoft Windows, such as `WinLogon` or `NetIQ Corporationms`.

Before running this script, run the ConfigRemoteServiceDown Knowledge Script to store a list of computers and services in the local repository on the target computer.

After you run ConfigRemoteServiceDown on each target computer in a group, you can use RemoteServiceDownLR in a monitoring policy for the group. On each computer, RemoteServiceDownLR knows what to monitor because ConfigRemoteServiceDown has stored that information in the local repository.

This script displays event information even if the remote computer is in maintenance mode.

Note
The AppManager agent does not need to be installed on the remote computer you want to monitor, nor does the remote computer need to exist in the TreeView pane of the Operator Console.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if a service is down. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns service status. The default is n.
Collect data only on service down?	Set to **y** to collect data only when a service is down. If enabled, and if the *Collect data?* parameter is also enabled, this script returns a value of 0 to indicate that a service is down. The default is n.
Auto-start service?	Set to **y** to automatically restart down services. The default is y.
Event severity when service down; auto-start failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and auto-start failed. The default is 5 (red event indicator).
Event severity when service down; auto-start succeeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and auto-start succeeded. The default is 25 (blue event indicator).

Description	How to Set It
Event severity when service down; auto-start disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and you have selected not to restart it. The default is 18 (yellow event indicator).
Event severity level for service not found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a selected service cannot be found. The default is 8 (red event indicator).

Report_CPULoad

Use this Knowledge Script to generate a detailed report about CPU usage and queue length. Using this report, you can aggregate the data by minute, hour, or day, and calculate statistics for each period, for example, the average value per hour.

This report uses data collected by the CpuLoaded script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all the data streams on a single page The default is By computer.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregation by	Select the time period by which the data in your report is presented. Select **Minute**, **Hour**, or **Day**. The default is Hour.
Aggregation interval	Specify the intervals to use to aggregate the data in the report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a **Table** or **Chart** of data stream values in the report, or choose **Both**. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder name is NT_CPULoad.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. The job ID helps you correlate a specific instance of a Report script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title for your report is NT CPU Load.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_CPULoadSummary

Use this Knowledge Script to generate a summary report about CPU usage and queue length. Using this report, you can make a statistical analysis of the data point values, for example, the average or maximum value over a period.

This report uses data collected by the CpuLoaded script.

Resource Objects

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Select the style	Select the style for the first page of your report: • **By computer** displays one value for each computer you selected. • **By legend** displays one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** displays one value for each unique legend from each computer. The default is By computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the time range of the report. • **Minimum**. The minimum value of data points for the time range of the report. • **Maximum**. The maximum value of data points for the time range of the report. • **Min/Avg/Max**. The minimum, average, and maximum values of data points for the time range of the report. • **Range**. The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**. The measure of how widely values are dispersed from the mean. • **Sum**. The total value of data points for the time range of the report. • **Close**. The last value for the time range of the report. • **Change**. The difference between the first and last values for the time range of the report (close - open = change). • **Count**. The number of data points for the time range of the report. The default is Average.
Select sorting or display options	Specify whether to sort data in your report or how to display the data: • **No sort**. Data is not sorted. • **Sort**. Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top %**. Chart only the top N % of selected data (sorted by default). • **Top N**. Chart only the top N of selected data (sorted by default). • **Bottom %**. Chart only the bottom N % of data (sorted by default). • **Bottom N**. Chart only the bottom N of selected data (sorted by default). The default is No sort.
Percentage (%) or count for top or bottom of chart	Specify a number for either the percent or count defined in *Select sorting or display options* (for example, Top 10%, or Top 10). The default is 25.
Truncate top or bottom?	Set to **yes** to truncate the top or bottom data in your report. If set to yes, the data table displays only the top or bottom N or % (for example, only the top 10%). If set to no, the table displays all data. The default is no.
Show totals on the table?	Set to **yes** to display additional calculations for each column of numbers in a table. If enabled, the following values are listed at the end of the table: • **Report Average**. An average of all values in a column. • **Report Minimum**. The minimum value in a column. • **Report Maximum**. The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for the report's output folder. The default folder prefix is NT_CPULoadSummary.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to add the job ID to the name of the output folder. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT CPU Load Summary.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_CPUResource

Use this Knowledge Script to generate a detailed report about the use of CPU resources, including the number of active processes, threads, and interrupts per second, and the utilization of CPU resources in user mode. Using this report, you can aggregate the data by minute, hour, or day, and calculate statistics for each period, for example, the average value per hour.

This report uses data collected by the CpuResource script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers. Each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer. • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all the data streams on a single page The default is By computer.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregation by	Select the time period by which the data in your report is presented. Select **Minute**, **Hour**, or **Day**. The default is Hour.
Aggregation interval	Specify the intervals to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_CPUResource.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT CPU Resource.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_CPUResourceSummary

Use this Knowledge Script to generate a summary report about the use of CPU resources, including the number of active processes, threads, and interrupts per second, and the utilization of CPU resources in user mode. Using this report, you can develop a statistical summary of the data you select, for example, the average value of data points over the period you define for the report.

This report uses data collected by the CpuResource script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Select the style	Select the style for the first page of your report: • **By computer** displays one value for each computer you selected. • **By legend** displays one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** displays one value for each unique legend from each computer. The default is By computer and legend.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the time range of the report. • **Minimum**. The minimum value of data points for the time range of the report. • **Maximum**. The maximum value of data points for the time range of the report. • **Min/Avg/Max**. The minimum, average, and maximum values of data points for the time range of the report. • **Range**. The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**. The measure of how widely values are dispersed from the mean. • **Sum**. The total value of data points for the time range of the report. • **Close**. The last value for the time range of the report. • **Change**. The difference between the first and last values for the time range of the report (close - open = change). • **Count**. The number of data points for the time range of the report. The default is Average.
Select sorting or display options	Specify whether to sort data in your report or how to display the data: • **No sort**. Data is not sorted. • **Sort**. Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top %**. Chart only the top N % of selected data (sorted by default). • **Top N**. Chart only the top N of selected data (sorted by default). • **Bottom %**. Chart only the bottom N % of data (sorted by default). • **Bottom N**. Chart only the bottom N of selected data (sorted by default). The default is No sort.
Percentage (%) or count for top or bottom of chart	Specify a number for either the percent or count defined in *Select sorting or display options* (for example, Top 10%, or Top 10). The default is 25.
Truncate top or bottom?	Set to **yes** to truncate the top or bottom data in your report. If set to yes, the data table displays only the top or bottom N or % (for example, only the top 10%). If set to no, the table displays all data. The default is no.
Show totals on the table?	Set to **yes** to display additional calculations for each column of numbers in a table. If set to yes, the following values are listed at the end of the table: • **Report Average**. An average of all values in a column. • **Report Minimum**. The minimum value in a column. • **Report Maximum**. The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_CPUResourceSummary.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT CPU Resource Summary.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_CPUUsageofProcessesSummary

Use this Knowledge Script to generate a summary report about CPU usage per named process, and total CPU usage by all named processes. Processes are named when you configure the CpuByProcess script. Using this report, you can develop a statistical summary of the data you select, for example, the average value of data points over the period you define for the report.

This report uses data collected by the CpuByProcess script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Select the style	Select the style for the first page of your report: • **By computer** displays one value for each computer you selected. • **By legend** displays one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** displays one value for each unique legend from each computer. The default is By computer and legend.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the time range of the report. • **Minimum**. The minimum value of data points for the time range of the report. • **Maximum**. The maximum value of data points for the time range of the report. • **Min/Avg/Max**. The minimum, average, and maximum values of data points for the time range of the report. • **Range**. The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**. The measure of how widely values are dispersed from the mean. • **Sum**. The total value of data points for the time range of the report. • **Close**. The last value for the time range of the report. • **Change**. The difference between the first and last values for the time range of the report (close - open = change). • **Count**. The number of data points for the time range of the report. The default is Average.
Select sorting or display options	Specify whether to sort data in your report or how to display the data: • **No sort**. Data is not sorted. • **Sort**. Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top %**. Chart only the top N % of selected data (sorted by default). • **Top N**. Chart only the top N of selected data (sorted by default). • **Bottom %**. Chart only the bottom N % of data (sorted by default). • **Bottom N**. Chart only the bottom N of selected data (sorted by default). The default is No sort.
Percentage (%) or count for top or bottom of chart	Specify a number for either the percent or count defined in *Select sorting or display options* (for example, Top 10%, or Top 10). The default is 25.
Truncate top or bottom?	Set to **yes** to truncate the top or bottom data in your report. If set to yes, the data table displays only the top or bottom N or % (for example, only the top 10%). If set to no, the table displays all data. The default is no.
Show totals on the table?	Set to **yes** to display additional calculations for each column of numbers in a table. If set to yes, the following values are listed at the end of the table: • **Report Average**. An average of all values in a column. • **Report Minimum**. The minimum value in a column. • **Report Maximum**. The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_CPUUsageofProcessesSummary.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT CPU Usage of Processes Summary.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_FilesOpen

Use this Knowledge Script to generate a report about the number of files open during a specified period. Using this report, you can aggregate data by minute, hour, or day, and calculate statistics for each period, for example, the average value per hour.

This report uses data collected by the FilesOpen script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all the data streams on a single page The default is By computer.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregation by	Select the time period by which the data in your report is presented. Select **Minute**, **Hour**, or **Day**. The default is Hour.
Aggregation interval	Specify the intervals to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_FilesOpen.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters.The default title is NT Files Open.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of the report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_LogicalDiskAvailSummary

Use this Knowledge Script to generate a summary report about the amount of free space (in MB) on a logical disk. Using this report, you can develop a statistical summary of the data you select, for example, the average value of data points over the period you define for the report.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Select the style	Select the style for the first page of your report: • **By computer** displays one value for each computer you selected. • **By legend** displays one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** displays one value for each unique legend from each computer. The default is By computer and legend.
Data settings	
Statistics to show	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the time range of the report. • **Minimum**. The minimum value of data points for the time range of the report. • **Maximum**. The maximum value of data points for the time range of the report. • **Min/Avg/Max**. The minimum, average, and maximum values of data points for the time range of the report. • **Range**. The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**. The measure of how widely values are dispersed from the mean. • **Sum**. The total value of data points for the time range of the report. • **Close**. The last value for the time range of the report. • **Change**. The difference between the first and last values for the time range of the report (close - open = change). • **Count**. The number of data points for the time range of the report. The default is Average.

Description	How to Set It
Select sorting or display options	Specify whether to sort data in your report or how to display the data: • **No sort**. Data is not sorted. • **Sort**. Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top %**. Chart only the top N % of selected data (sorted by default). • **Top N**. Chart only the top N of selected data (sorted by default). • **Bottom %**. Chart only the bottom N % of data (sorted by default). • **Bottom N**. Chart only the bottom N of selected data (sorted by default). The default is No sort.
Percentage (%) or count for top or bottom of chart	Specify a number for either the percent or count defined in *Select sorting or display options* (for example, Top 10%, or Top 10). The default is 25.
Truncate top or bottom?	Set to **yes** to truncate the top or bottom data in your report. If set to yes, the data table displays only the top or bottom N or % (for example, only the top 10%). If set to no, the table displays all data. The default is no.
Show totals on the table?	Set to **yes** to display additional calculations for each column of numbers in a table. If set to yes, the following values are listed at the end of the table: • **Report Average**. An average of all values in a column. • **Report Minimum**. The minimum value in a column. • **Report Maximum**. The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_LogicalDiskAvailSummary.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT Logical Disk Available Summary.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).

Description	How to Set It
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_LogicalDiskUsageSummary

Use this Knowledge Script to generate a summary report about the percentage of disk space used and the amount of free space (in MB). Using this report, you can develop a statistical summary of the data you select, for example, the average value of data points over the period you define for the report.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Select the style	Select the style for the first page of your report: • **By computer** displays one value for each computer you selected. • **By legend** displays one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** displays one value for each unique legend from each computer. The default is By computer and legend.
Data settings	
Statistics to show	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the time range of the report. • **Minimum**. The minimum value of data points for the time range of the report. • **Maximum**. The maximum value of data points for the time range of the report. • **Min/Avg/Max**. The minimum, average, and maximum values of data points for the time range of the report. • **Range**. The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**. The measure of how widely values are dispersed from the mean. • **Sum**. The total value of data points for the time range of the report. • **Close**. The last value for the time range of the report. • **Change**. The difference between the first and last values for the time range of the report (close - open = change). • **Count**. The number of data points for the time range of the report. The default is Average.

Description	How to Set It
Select sorting or display options	Specify whether to sort data in your report or how to display the data: • **No sort**. Data is not sorted. • **Sort**. Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top %**. Chart only the top N % of selected data (sorted by default). • **Top N**. Chart only the top N of selected data (sorted by default). • **Bottom %**. Chart only the bottom N % of data (sorted by default). • **Bottom N**. Chart only the bottom N of selected data (sorted by default). The default is No sort.
Percentage (%) or count for top or bottom of chart	Specify a number for either the percent or count defined in *Select sorting or display options* (for example, Top 10%, or Top 10). The default is 25.
Truncate top or bottom?	Set to **yes** to truncate the top or bottom data in your report. If set to yes, the data table displays only the top or bottom N or % (for example, only the top 10%). If set to no, the table displays all data. The default is no.
Show totals on the table?	Set to **yes** to display additional calculations for each column of numbers in a table. If set to yes, the following values are listed at the end of the table: • **Report Average**. An average of all values in a column. • **Report Minimum**. The minimum value in a column. • **Report Maximum**. The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_LogicalDiskUsageSummary.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT Logical Disk Usage Summary.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).

Description	How to Set It
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_MemoryUtilization

Use this Knowledge Script to generate a report about the use of physical and virtual memory, and paging files. Using this report, you can aggregate data by minute, hour, or day, and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the MemUtil script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all the data streams on a single page The default is By computer.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregation by	Select the time period by which the data in your report is presented. Select **Minute**, **Hour**, or **Day**. The default is Hour.
Aggregation interval	Specify the intervals to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_MemoryUtilization.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT Memory Utilization.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_MemoryUtilizationSummary

Use this Knowledge Script to generate a summary report about the use of physical and virtual memory, and paging files. Using this report, you can develop a statistical summary of the data you select, for example, the average value of data points over the period you define for the report.

This report uses data collected by the MemUtil script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Select the style	Select the style for the first page of your report: • **By computer** displays one value for each computer you selected. • **By legend** displays one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** displays one value for each unique legend from each computer. The default is By computer and legend.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the time range of the report. • **Minimum**. The minimum value of data points for the time range of the report. • **Maximum**. The maximum value of data points for the time range of the report. • **Min/Avg/Max**. The minimum, average, and maximum values of data points for the time range of the report. • **Range**. The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**. The measure of how widely values are dispersed from the mean. • **Sum**. The total value of data points for the time range of the report. • **Close**. The last value for the time range of the report. • **Change**. The difference between the first and last values for the time range of the report (close - open = change). • **Count**. The number of data points for the time range of the report. The default is Average.
Select sorting or display options	Specify whether to sort data in your report or how to display the data: • **No sort**. Data is not sorted. • **Sort**. Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top %**. Chart only the top N % of selected data (sorted by default). • **Top N**. Chart only the top N of selected data (sorted by default). • **Bottom %**. Chart only the bottom N % of data (sorted by default). • **Bottom N**. Chart only the bottom N of selected data (sorted by default). The default is No sort.
Percentage (%) or count for top or bottom of chart	Specify a number for either the percent or count defined in *Select sorting or display options* (for example, Top 10%, or Top 10). The default is 25.
Truncate top or bottom?	Set to **yes** to truncate the top or bottom data in your report. If set to yes, the data table displays only the top or bottom N or % (for example, only the top 10%). If set to no, the table displays all data. The default is no.
Show totals on the table?	Set to **yes** to display additional calculations for each column of numbers in a table. If set to yes, the following values are listed at the end of the table: • **Report Average**. An average of all values in a column. • **Report Minimum**. The minimum value in a column. • **Report Maximum**. The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_MemoryUtilizationSummary.

Description	How to Set It
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT Memory Utilization Summary.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_NetworkBusy

Use this Knowledge Script to generate a report about the use of bandwidth on network interface cards. Using this report, you can aggregate data by minute, hour, or day, and calculate statistics for each period, for example, the average value per hour.

This report uses data collected by the NetworkBusy script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all the data streams on a single page The default is By computer.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregation by	Select the time period by which the data in your report is presented. Select **Minute**, **Hour**, or **Day**. The default is Hour.
Aggregation interval	Specify the intervals to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_NetworkBusy.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT Network Busy.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_PagingHigh

Use this Knowledge Script to generate a report about the number of reads and writes per second to the pagefile. Using this report, you can aggregate data by minute, hour, or day, and calculate statistics for each period, for example, the average value per hour.

This report uses data collected by the PagingHigh script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all the data streams on a single page The default is By computer.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregation by	Select the time period by which the data in your report is presented. Select **Minute**, **Hour**, or **Day**. The default is Hour.
Aggregation interval	Specify the intervals to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_PagingHigh.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT Paging High.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_PhysicalDiskIO

Use this Knowledge Script to generate a report about the number of reads, writes, and transfers per second for a physical disk. Using this report, you can aggregate data by minute, hour, or day, and calculate statistics for each period, for example, the average value per hour.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all the data streams on a single page The default is By computer.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregation by	Select the time period by which the data in your report is presented. Select **Minute**, **Hour**, or **Day**. The default is Hour.
Aggregation interval	Specify the intervals to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_PhysicalDiskIO.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters.The default title is NT Physical Disk IO.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_PhysicalDiskQueueLength

Use this Knowledge Script to generate a report about physical disk queue length. Using this report, you can aggregate data by minute, hour, or day, and calculate statistics for each period, for example, the average value per hour.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all the data streams on a single page The default is By computer.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregation by	Select the time period by which the data in your report is presented. Select **Minute**, **Hour**, or **Day**. The default is Hour.
Aggregation interval	Specify the intervals to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_PhysicalDiskQueueLength.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. By default, the job ID is not included. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT Physical Disk Queue Length.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_PrinterHealth

Use this Knowledge Script to generate a report about printer health. Printer health is determined by whether or not the printer is paused, and the queue length for printer jobs. Using this report, you can aggregate data by minute, hour, or day, and calculate statistics for each period, for example, the average value per hour.

This report uses data collected by the PrinterHealth script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all the data streams on a single page The default is By computer.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregation by	Select the time period by which the data in your report is presented. Select **Minute**, **Hour**, or **Day**. The default is Hour.
Aggregation interval	Specify the intervals to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_PrinterHealth.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. By default, the job ID is not included. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT Printer Health.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_Process

Use this Knowledge Script to generate a report about the number of processes running during a specified period. Using this report, you can aggregate data by minute, hour, or day, and calculate statistics for each period, for example, the average value per hour.

This report uses data collected by the Processes script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all the data streams on a single page The default is By computer.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Select peak weekday(s)	Select the days of the week to include in your report. The default is every day of the week.
Aggregation by	Select the time period by which the data in your report is presented. Select **Minute**, **Hour**, or **Day**. The default is Hour.
Aggregation interval	Specify the intervals to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Specify whether to include a table or chart, or both, of data stream values in the report. The default is Table.
Select chart style	Select the graphic properties for the charts in your report. The default chart style is Bar.
Select output folder	Select the parameters for your report's output folder. The default folder prefix is NT_Process.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters. The default title is NT Process.
Add time stamp to title?	Set to **yes** to add a time stamp to the title of your report, making each title unique. The time stamp shows the date and time the report was generated. The default is no. A time stamp lets you run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_TopCPUProcs

Use this Knowledge Script to generate a report about the total CPU used by all processes and which processes consume the most CPU resources.

This report uses data collected by the TopCpuProcs script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report. **Note** For this report, select only one View, and up to 15 computers or server groups. The data wizard allows you to select more, but if you do, the Finish button is disabled. This mechanism prevents you from selecting too much data for the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Select output folder	Select the parameters for your report's output folder. The default prefix for the folder name is NT_TopCPUProcs.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

Report_TopMemoryProcs

Use this Knowledge Script to generate a report about the total memory used by all processes and which processes consume the most memory resources.

This report uses data collected by the TopMemoryProcs script.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers whose data you want to include in your report. **Note** Select only one View, and up to 15 computers or server groups. The data wizard allows you to select more, but if you do, the Finish button is disabled. This mechanism prevents you from selecting too much data for the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Select output folder	Select the parameters for your report's output folder. The default prefix for the folder name is NT_TopMemoryProcs.
Add job ID to output folder name?	Set to **yes** to add the job ID to the report's output folder name. The default is no. A job ID lets you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Provide a name for the report and set any other report parameters.
Event notification	
Event for report success?	Set to **yes** to raise an event if the report is successfully generated. The default is yes.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35 (magenta event indicator).
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25 (blue event indicator).
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation fails. The default is 5 (red event indicator).

RunAwayProcesses

Use this Knowledge Script to detect runaway processes on the specified computer by repeatedly sampling CPU usage for processes. This script raises an event if a process exceeds the CPU usage threshold in the number of consecutive samples taken (one at each interval).

For example, if this script detects that the process `cmd` has exceeded the CPU usage threshold for five consecutive monitoring periods, it might indicate that the process is trapped in an infinite loop or has encountered other problems. In addition to raising an event to notify you of the problem, you can stop any detected runaway processes. The detail message shows the list of processes being sampled.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if a process exceeds the CPU usage threshold in the number of consecutive samples taken (one at each interval). The default is y.
Collect data?	Set to **y** to collect data for charts and reports. When enabled, data collection returns the CPU usage for runaway processes. The default is n.
Maximum CPU usage threshold for runaway processes	Specify the maximum percentage of CPU time any process can be using when sampled before an event is raised. The default is 90%.
Number of consecutive samples	Specify the number of consecutive samples to take before raising an event. The default is 3.
Number of runaway processes	Specify the number of processes to display in a detail event or data message. Type 0 for all processes. The default is 5.
Ignore these processes	Specify the names of any processes to exclude from sampling. Separate the names with commas (,) and no space. The default is `SQLSERVR`.
Never kill these processes	Specify the names of any processes that should never be stopped. Separate the names with commas (,) and no spaces. The default is `EXPLORER,NetIQmc,NetIQccm,NetIQms,SERVICES,LSASS,WINLOGON,svchost`. If you stop these processes, your computer restarts.
Kill runaway process when detected?	Set to **y** to automatically stop a process. AppManager does not stop any process you specify in the *Never kill these processes* parameter. The default is n.
Event severity level for runaway processes detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a runaway process is detected. The default is 5 (red event indicator).

Description	How to Set It
Event severity level for killed runaway process	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a runaway process is stopped. The default is 10 (red event indicator).
Event severity level for failed to kill runaway process	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a runaway process cannot be stopped. The default is 10 (red event indicator).

ServerBusy

Use this Knowledge Script to monitor Windows server activity for network clients. This script raises an event if the number of active sessions or the number of open files exceeds the threshold you specify.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the number of active sessions or the number of open files exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. When enabled, data collection returns the number of active sessions and the number of open files. The default is n.
Maximum number of active sessions threshold	Specify the maximum number of client computers that can be connected to the server before an event is raised. The default is 50.
Maximum number of opened files threshold	Specify the maximum number of files that can be opened by network clients before an event is raised. The default is 200.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ServerBytes

Use this Knowledge Script to monitor the rate of bytes transferred to and from the target computer. Because the transfer rate can vary dramatically depending on the activity being performed, you can click the **Advanced** tab and set the number of consecutive occurrences to a value greater than 1 to filter out insignificant spikes. The detail message includes the number of bytes sent and received per second.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the number of bytes transferred per second exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. When enabled, data collection returns the number of bytes transferred per second. The default is n.
Maximum bytes transferred per second threshold	Specify the maximum number of bytes that can be transferred (sent and received) per second before an event is raised. The default is 800,000 bytes.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of bytes transferred per second exceeds the threshold. The default is 25 (blue event indicator).

ServerError

Use this Knowledge Script to monitor the number of sessions that errored out during the monitoring interval. This script tracks only the number of sessions that failed and were closed and dropped in an error state since the last time the script ran (delta value). This script raises an event if the number of the errored-out sessions exceeds the threshold you specify.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the number of errored-out sessions exceeds the threshold. The default is n.
Collect data?	Set to **y** to collect data for charts and reports. When enabled, data collection returns the number of errored-out sessions. The default is n.
Maximum errored-out sessions threshold	Specify the maximum number of errored-out sessions allowed before an event is raised. The default is 2.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8 (red event indicator).

ServerTimeout

Use this Knowledge Script to monitor the number of sessions that timed out during the monitoring interval. To conserve resources, Windows servers automatically disconnect sessions that are idle for a set period. If a session's idle time exceeds the autodisconnect parameter for the server, the session times out and is closed. This script tracks the number of sessions that timed out since the last time the script ran (delta value) and raises an event if the number of the timed-out sessions exceeds the threshold you specify.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the number of the timed-out sessions exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. When enabled, data collection returns the number of timed-out sessions. The default is n.
Maximum timed-out sessions threshold	Specify the maximum number of timed-out sessions allowed before an event is raised. The default is 2.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 25 (blue event indicator).

ServiceChange

Use this Knowledge Script to detect changes to the status and startup type of Windows services. This script raises an event if the status (such as running, stopped, or pending), or startup type (such as manual, automatic, or disabled) of any service changes. For example, this script raises an event if a service startup type changes from Automatic to Manual.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the status or startup type of any service changes. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- service is unchanged, or • **0** -- service is not running or has changed. The default is n.
Services	Specify the names of the services you want to monitor, separating multiple names with commas (,) and no spaces. You can specify the internal service names or the service names displayed in the Control Panel. Type an asterisk (*) to check all services marked "Automatic." The default is EventLog.
Event severity level for service start-type changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service start-type changes. The default is 10 (red event indicator).
Event severity level for service status changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service status changes. The default is 5 (red event indicator).
Event severity level for failed to retrieve service information	Set the event severity level, from 1 to 40, to indicate the importance of an event in which service information cannot be retrieved. The default is 18 (yellow event indicator).

ServiceDown

Use this Knowledge Script to monitor whether specified Microsoft Windows services are stopped or started, and, optionally, start any service that is stopped. This script allows you to monitor Windows Services that are not discovered by AppManager for Microsoft Windows, such as the `WinLogon` or `NetIQms` services.

Tip
Use the General_ServiceDown script to monitor services that are discovered by AppManager.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ServiceDown job fails unexpectedly. The default is 5 (red event indicator).
Monitor Services	
Services to monitor	Specify the names of the services you want to monitor, separating multiple names with commas. For example: `MSSQLServer,SQLServerAgent,PrintSpooler`. The default is `EventLog,WinMgmt`. You can specify both long and short service names, the internal service names, or the service names displayed in the Control Panel. Type an asterisk (`*`) to monitor all service startup types specified in the *Service start-type filter* parameter.
Service start-type filter	Select the startup type (All, Automatic, Manual, Disabled) for the services you want to monitor. Use this parameter along with the *Services to monitor* parameter to monitor services by their startup types instead of their names. For example, if you enter "`*`" in the *Services to monitor* parameter and then select **Manual**, the script monitors all services whose startup type is Manual. The default is Automatic. **Notes** • The script uses this parameter only when you enter an asterisk (`*`) in the *Services to monitor* parameter. • Be careful when using an asterisk (`*`) in the *Services to monitor* parameter along with the **Manual** option. In this situation, if you also select the *Also start services that were last stopped normally* parameter, AppManager starts all Manual services.

Description	How to Set It
Services to exclude	Specify the names of the services you want to exclude from monitoring, separating multiple names with commas. You can specify the internal service names or the service names displayed in the Control Panel.
Start services that stopped abnormally?	Select **Yes** to automatically start services that stopped abnormally. The default is Yes.
Also start services that were last stopped normally?	Select **Yes** to automatically start a service that stopped normally, perhaps as the result of a stop request from another process or human interaction. The default is unselected.
Service start timeout	Set the maximum number of seconds to wait after initiating the start command before reporting that the service could not be started. If the service is not running after the specified amount of time, this script reports that the service did not start in the time you specified. The default is 30 seconds.
Monitor Dependent Services	
Monitor dependent services?	Select **Yes** to monitor services that are dependent upon the other services you chose to monitor. The default is Yes.
Start dependent services?	Select **Yes** to automatically start a stopped service that is dependent upon a stopped monitored service. AppManager starts dependent services after the monitored service is started. The default is unselected. The options you choose for start-type filter and service start timeout apply to dependent services as well. **Note** If you enable this parameter, you must also enable the *Monitor dependent services?* parameter.
Event Notification	
Raise event if a service is stopped and should not be started?	Select **Yes** to raise an event if a service is stopped and this script is not set to start the service. The default is Yes.
Event severity when a service is stopped and should not be started	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a stopped service is not set to be started. The default is 5 (red event indicator).
Raise event if a service is stopped and cannot be started?	Select **Yes** to raise an event if a service is stopped and this script cannot start the service. The default is Yes.
Event severity when a service is stopped and cannot be started	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a stopped service cannot be started. The default is 10 (red event indicator).
Raise event if a stopped service is started successfully?	Select **Yes** to raise an event if AppManager successfully starts a stopped service. The default is Yes.
Event severity when a stopped service is started successfully	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully starts a stopped service. The default is 25 (blue event indicator).
Raise event if a service was last stopped normally?	Select **Yes** to raise an event if a service was last stopped normally. If enabled, an event is raised only if *Also start services that were last stopped normally* is not selected. The default is Yes.
Event severity when a services was last stopped normally	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service stopped normally and was not set to be started. The default is 30 (blue event indicator).
Raise event if a monitored service does not exist?	Select **Yes** to raise an event if a service specified in the *Services to monitor* parameter does not exist. The default is Yes.

Description	How to Set It
Event severity when a monitored service does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service cannot be found. The default is 8 (red event indicator).
Raise event if a monitored service is disabled?	Select **Yes** to raise an event if a service is disabled. The default is Yes. AppManager cannot automatically start disabled services.
Event severity when a monitored service is disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service is disabled. The default is 12 (yellow event indicator).
Data Collection	
Collect data for monitored services?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns a separate data stream for each service you monitor: • **100** -- the service is started • **0** -- the service is stopped • **50** -- the service is stopped and was successfully started The data detail message includes the name of the service, the start type, and the status. The default is unselected.
Collect data for dependent services?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns a separate data stream for each dependent service you monitor: • **100** -- the service is started • **0** -- the service is stopped • **50** -- the service is stopped and was successfully started The data detail message includes the name of the dependent service, the start type, and the status. The default is unselected.

ServiceDownLR

Use this Knowledge Script to detect whether specified services on the computer on which you run the script are down. A service detected as down can be restarted.The Windows services include those that are not discovered by AppManager for Microsoft Windows, such as `WinLogon` or `NetIQms`.

This script requires that you first use the ConfigServiceDown Knowledge Script to store a list of services in the local repository on the computer where ServiceDownLR runs.

Once you have run ConfigServiceDown on each computer in a group, you can use ServiceDownLR in a monitoring policy for the group. On each computer, ServiceDownLR knows what to monitor because ConfigServiceDown previously stored that information in the local repository.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if any service is down?	Set to **y** to raise an event if services are down. The default is y.
Collect data for service status?	Set to **y** to collect data for charts and reports. If enabled, data collection returns a separate data stream for each service you monitor: • **100** -- the service is started • **0** -- the service is stopped • **50** -- the service is stopped and was successfully started The data detail message includes the name of the service, the start type, and the status. The default is n.
Collect data only on service down?	Set to **y** to collect data only when a service is down. If set to y, returns a value of 0. Enable this parameter only if the *Collect data?* parameter is enabled. The default is n.
Auto-start service?	Set to **y** to automatically restart down services. The default is y.
Event severity when service down; auto-start failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and auto-start fails. The default is 5 (red event indicator).
Event severity when service down; auto-start succeeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and auto-start succeeds. The default is 25 (blue event indicator).
Event severity when service down; auto-start disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and the *Auto-start service?* parameter is set to n. The default is 18 (yellow event indicator).

Description	How to Set It
Event severity when service not found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a specified service is not found. The default is 8 (red event indicator).
Event severity when Knowledge Script error occurs	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ServiceDownLR job fails unexpectedly. The default is 35 (magenta event indicator).

ServiceHung

Use this Knowledge Script to detect if a Windows service is hung. A hung service is a service in a Start-Pending, Stop-Pending, Continue-Pending, or Pause-Pending state for a number of consecutive intervals. This script raises an event if any service is detected as hung. The service can then be stopped or restarted.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if a service is detected as hung. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the service is up, or • **0** -- the service is hung. The default is n.
Services	Provide the names of the services you want to monitor, separating the names with commas (,) and no spaces. You can specify the internal service names or the service names displayed in the Control Panel. Type an asterisk (*) to check all services whose startup type is Automatic. The default is `EventLog`.
Maximum number of consecutive iterations before service is considered hung	Specify the maximum number of consecutive times a service can be in a Start-Pending, Stop-Pending, Continue-Pending, or Pause-Pending state before it is considered hung. The default is 2.
Kill the hung service?	Set to **y** to automatically stop hung services. The default is y.
Auto-start killed service?	Set to **y** to automatically restart the service after stopping it. The default is y.
Event severity level for auto-start failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is hung and an attempt to restart it was not successful. The default is 5 (red event indicator).
Event severity level for auto-start succeeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is hung and was restarted successfully. The default is 25 (blue event indicator).
Event severity level for don't auto-start	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is hung and the *Auto-start killed service?* parameter is disabled. The default is 18 (yellow event indicator).
Event severity level for failed to retrieve service status	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a specified service could not be found. The default is 10 (red event indicator).

Description	How to Set It
Event severity level for failed to kill service	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is hung and could not be stopped. The default is 10 (red event indicator).

ServiceRemove

Use this Knowledge Script to detect when Windows services are added or removed in the monitoring interval. This script raises an event when changes are made to the services installed on the target computer. The script monitors only changes in the list of automatic services (startup type), including installs and uninstalls of services in automatic startup and changing a service from automatic to disabled/manual or vice-versa.

Note
If a computer is restarted after a service is removed, the agent counters are reset. Once the counters are reset, AppManager cannot detect the service removal and does not raise an event.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event when changes are made to the services installed on the target computer. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of services currently installed. The default is n.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which service changes are detected. The default is 12 (yellow event indicator).

SharedFiles

Use this Knowledge Script to monitor and list shared files that are open. This script raises an event if the number of open shared files exceeds the threshold you specify. Run this script on the server that hosts the shared files.

Note
Before running this script, be sure the `netiqmc` service is set to run as a domain user account user in the same domain as (or a domain trusted by) the target computer. Use the Services Control Panel to identify an account for the service to run as.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is to **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the number of open shared files exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of shared files currently open. The detail message lists the shared files with file IDs and lock information. The default is n.
Maximum number of shared files open threshold	Specify the maximum number of shared files that can be open at one time before an event is raised. The default is 100.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of open shared files exceeds the threshold. The default is 8 (red event indicator).

SystemUpTime

Use this Knowledge Script to monitor the system up time for a Windows server or workstation. This script tracks the number of hours that the computer has been operational since it was last rebooted. This script raises an event if the computer was rebooted within the monitoring interval.

To monitor whether a computer has gone down for reasons other than being placed in maintenance mode, use the General_MachineDown Knowledge Script.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if the computer was rebooted within the monitoring interval. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of hours the system has been up. The default is n.
Event severity level for system reboot	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the computer was rebooted. The default is 8 (red event indicator).
Event severity level for an unexpected Knowledge Script error	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SystemUpTime job fails unexpectedly. The default is 35 (magenta event indicator).

TopCpuProcs

Use this Knowledge Script to monitor total CPU resources used by all processes and which processes consume the most CPU resources. This script raises an event if the percentage of CPU usage exceeds the threshold you specify. In addition, this script generates a data stream for processor usage.

Resource Object

CPU folder

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Create event if processor utilization is over the threshold?	Set to **Yes** to raise an event if the percentage of CPU time used exceeds the threshold you specify. The default is Yes.
Severity - Processor utilization over the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 10 (red event indicator).
Number of processes to include in detail message	Specify the number of top processes to display in the detail message (event or data). Enter 0 to display all processes. The default is 10. **Note** Limit the number of processes included in the detail message to the top five to ten processes. In most cases, including all processes increases the size of the detail message without providing much more useful information. Typically, the top few processes are the most significant and the most userful for troubleshooting purposes.
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the TopCpuProcs job fails unexpectedly. The default is 5 (red event indicator).
Data Collection	
Collect processor utilization data?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the process name, ID, and utilization percentage (%) for the number of processes you set in *Number of processes to include in detail message*. The default is unselected. **Note** If the value you set in *Number of processes to include in detail message* is greater than the number of processes running on the computer, the event detail message only contains the list of running processes; AppManager does not include blank lines to represent the non-running processes.
Monitoring	
Threshold -- Total processor utilization	Specify the maximum percentage of CPU resources that can be in use for all processes before an event is raised. The default is 85%.

TopMemoryProcs

Use this Knowledge Script to monitor total memory (in KB) usage for all processes and to identify which processes consume the most memory. This script raises an event if memory usage exceeds the threshold you specify. In addition, this script generates a data stream for memory utilization.

Resource Object

Memory folder

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Create event if memory utilization exceeds the threshold?	Select **Yes** to raise an event if memory usage exceeds the threshold you specify. The default is Yes.
Severity -- Memory utilization over the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. The default is 10 (red event indicator).
Number of processes to include in detail message	Specify the number of top processes to display in the detail message (event or data). Enter 0 to display all processes. The default is 10. **Note** Limit the number of processes included in the detail message to the top five to ten processes. In most cases, including all processes increases the size of the detail message without providing much more useful information. Typically, the top few processes are the most significant and the most useful for troubleshooting purposes.
Severity -- Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the TopMemoryProcs job fails unexpectedly. The default is 5 (red event indicator).
Data Collection	
Collect memory utilization data?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the process name, ID, and memory utilization (in KB), as well as job configuration information for each data point value. The default is unselected.
Monitoring	
Threshold -- Total memory utilization	Specify the maximum amount of memory that can be in use for all processes before an event is raised. The default is 5120 KB.
Threshold -- Size scale	Select the scale for the total memory utilization threshold you specify (kilobytes, megabytes, gigabytes, terabytes). The default is kilobytes.

TrustRelationship

Use this Knowledge Script to test the domain trust relationship from the computer where you run this script to a specified domain. The domain of the managed computer running this script is considered the *trusting* or resource domain. The domains you specify as script properties are the domains you expect to be trusted domains. This script raises an event if there are problems with the domain trust, such as when a trusted password is no longer valid or the Primary Domain Controller of the trusting domain cannot be located.

Note
Before running this script, be sure the `netiqmc` and `netiqccm` services are set to run as a domain user account with Administrator privileges in both the trusting and trusted domains. For example, to test whether Domain A still trusts Domain B, the agent services must run as an account with domain Administrator privileges in both Domain A and Domain B. Use the Services Control Panel to identify an account for the service to run as.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event?	Set to **y** to raise an event if there are problems with the domain trust relationships. The default is y.
Collect data?	Specify whether to collect data for charts and reports. If enabled, data collection returns: • **100** -- the domain of the managed computer trusts the domains entered, or • **0** -- the trust relationship is broken. The default is n.
Trusted domains	Provide a list of trusted domains, separated by commas with no spaces. Trusted domains contain resources that computers in other domains can use.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which there are problems with the domain trust relationships. The default is 8 (red event indicator).

UnixRemoteProcessDown

Use this Knowledge Script to monitor applications on remote UNIX computers where you cannot easily install a UNIX agent. This script uses a proxy UNIX agent, installed on another computer, to monitor processes on the remote UNIX computer.

If a monitored process is found to be down, this script can restart it automatically, using a script or command you supply. Be sure to read the help for the *Scripts or commands to restart processes* parameter before proceeding.

You can specify the process names to be monitored in the *Processes to monitor* parameter, or you can provide a configuration file in XML format to specify processes to monitor and what steps to take to restart them if they are down. For more information, see "Remote Process Monitoring Using a Configuration File" on page 3190.

Resource Object

UNIX Machine folder

Default Schedule

The default interval for this script is **Every 20 seconds**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if process is down?	Select **Yes** to raise an event if a monitored process is down. The default is Yes.
Event severity when process is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a process is down. The default is 10.
Raise event if process is running?	Select **Yes** to raise an event if a monitored process is running. The default is unselected.
Event severity when process is running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored process is running. The default is 25.
Remote Host Connection	
Configure access to the remote managed computers by specifying their root password. All of the remote computers must use the same root password. This script can use SSH with root password authentication or Telnet to communicate with the remote managed computer.	
Password for root user account	To use Secure Shell (SSH) for the connection to the remote computers, ensure that SSH with root authentication is enabled on the remote UNIX computers where you want to install the UNIX agent. For this parameter, specify the password for the root user to securely access the remote UNIX computers. This script does not support SSH root authentication with an RSA key.

Description	How to Set It

Connection Transport	This script can use SSH with root password authentication or Telnet to communicate with the remote managed computers.
	If you select the **Telnet/FTP** option (the default), the Telnet prompt on the remote computer must end with a space or one of the following characters: %, >, #, $
	The following is an example of a supported Telnet prompt:
	`user@hostname>`
	Here is an example of an unsupported Telnet prompt:
	`<user@hostname:/tmp - 2005-Mar-09>`
	`->`
	In the example above, the last character in the first line of the two-line prompt is a line feed character, which is not supported.

Telnet non-root user account	If you selected Telnet to connect to the remote UNIX computers, specify a non-root user account to use for the connection. When connecting to a remote UNIX computer using Telnet and FTP, this script switches from the non-root user to the root user.
Telnet non-root user account password	If you selected Telnet as the connection transport medium, specify the password for the non-root user account to connect to the remote UNIX computers.
Monitoring Source Configuration	
Full path to configuration file for remote monitoring	Supply a full directory path to an XML file to use for communications with the remote UNIX computer. The default is c:\temp\`config.xml`
Manual Configuration	
Hostnames or IP addresses where processes are to be monitored	Supply a list of hostnames or IP addresses of the UNIX computers where processes are to be monitored. Separate multiple hostnames with commas (,) and no spaces. Supply IP addresses in dotted notation, such as 23.45.678.9. Separate multiple IP addresses with commas and no spaces.
Processes to monitor	Supply the names of the UNIX application processes to monitor. Separate multiple process names with commas and no spaces. You can also enter a Perl regular expression here if you want to exclude and include processes on various platforms using one argument. See Running this Knowledge Script for more information.

Description	How to Set It
Scripts or commands to restart processes (comma-separated	Supply one of the following: • a list of full directory paths to script files to use to restart any processes that are found to be down, or • a list of commands to use to restart these processes. There is no need to supply a value for this parameter if you specify "n" for the *Restart process if down?* parameter. If you configure this script to restart a process, specify a list of restart commands or shell scripts that contain the restart commands. Do not execute restart commands in the foreground. When executing a restart command in the foreground, this script cannot run at its next scheduled interval until after all the restart commands have completed. When specifying: • A list of commands to run on the remote computer, run each command in the background by adding an ampersand (&) and separating each command with a comma. If this script is configured to use Telnet/FTP, you can restart a process in the background by adding an ampersand (&) to each command. If this script is configured to use SSH/SFTP, use a shell script on the remote computer to restart the processes in the background and ensure that `stdout` and `stderr` are redirected to a log file. When configured to use SSH/SFTP, this script always executes a command to restart a process in the foreground. • A shell script on the remote computer that restarts the processes you want, in the shell script, add an ampersand (&) to each restart command—and ensure that `stdout` and `stderr` are redirected to a log file—to restart a process in the background.
Restart process if down? (y/n for each process, comma-separated)	Provide a list specifying "y" or "n" for each process in the *Processes to monitor* parameter. Specify y for a process if you want this script to restart it on the remote computer if it is found to be down. The commands or scripts you specified for the previous parameter will be used. Separate the list of Ys and Ns with commas and no spaces.

Running this Knowledge Script

The UnixRemoteProcessDown script requires the proxy UNIX agent to run as the root user account. To enable this script, you must run the AppManager installation program (the `AMxx_UNIX_setup.exe` file) on the proxy computer. An extra "helper" file will be installed: `UnixRemoteProcessDown.exe`.

To use this script to monitor the up and down status of the UNIX agent, specify `nqmagt` in the list of processes to monitor. If the `nqmagt` process is down, you can specify a restart command to restart the agent:

```
/etc/init.d/nqmdaemon start
```

This script can use either the Secure Shell (SSH) program with root password authentication or Telnet to make a secure connection to the remote UNIX computer. By default, Telnet is used, but you can select SSH/SFTP from the *Connection Transport* parameter to use Secure Shell instead. If you choose to use Telnet, you must supply a non-root user account name and password.

Note
Proxy monitoring with this script is possible only if the SSH program is installed on the target computer, or if the Telnet protocol is enabled on it.

You can also supply a Perl regular expression for the *Names of processes to monitor* parameter to check for a specific string. For example, you can exclude and include processes on various platforms using one argument. A process may be running out of the `/usr`, the `/opt`, or the `/var` directory, but you are not sure where. Or perhaps a process is running out of different locations on different platforms. If you enter

```
(/usr|/opt)/[processname]
```

for the *Names of processes to monitor* parameter, the script would monitor the process that is running in `/usr` OR in `/opt` but NOT in `/var`.

Remote Process Monitoring Using a Configuration File

The UnixRemoteProcessDown script includes an option to use a configuration file in XML format to supply monitoring instructions to the agent. In such a file, you can supply a list of processes to monitor on a given remote UNIX computer, specify how to restart these processes, and indicate whether to restart these processes.

By default, the script looks for the following configuration file:

```
c:\temp\config.xml
```

However, you can supply a different file as the value for the *Full path to configuration file for remote monitoring* parameter.

Following is an example of a valid XML configuration file that tells the UNIX agent which processes to monitor and what to do if the processes are not running:

```
 <?xml version="1.0" encoding="utf-8" ?>
<SERVERS>
  <SERVER name="uws3">
    <PROCESS name="nqmagt" startupscript="/etc/init.d/nqmdaemon start" restart="y"/>
<PROCESS name="xntpd"  startupscript="/etc/init.d/xntpd start" restart="n"/>
</SERVER>
  <SERVER name="uws19">
     <PROCESS name="inetd"  startupscript="/etc/init.d/inetsvc start" restart="n"/>
<PROCESS name="init"  startupscript="/etc/init.d/init start" restart="n"/>
</SERVER>
       </SERVERS>
```

Chapter 54
NTAdmin Knowledge Scripts

The NTAdmin category provides Knowledge Scripts for performing Windows administrative tasks or special one-time activities. To run Knowledge Scripts in this category, you need to be defined as a user with administrator privileges on the computer on which you run the scripts.

Some Knowledge Scripts perform AppManager administrative tasks or operations that should be restricted to a limited number of users. To control access to these Knowledge Scripts, the scripts are only made available to users who are assigned to the Administrator role through AppManager Security Manager.

Most of the administrative Knowledge Scripts are in the Action, AMAdmin, and NTAdmin categories, and by default these Knowledge Scripts are designated as being for administrators only. For more information, see the *Administrator Guide for AppManager*.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AddGroup	Adds a local or domain Windows group account.
AddGroupViaAD	Adds a domain group account to Active Directory.
AddUser	Adds a local or domain Windows user account.
AddUserViaAD	Adds a domain user account to Active Directory.
ChangePassword	Changes the password for a specified local or domain user account.
CheckServicePack	Compares the Windows service pack level on a managed computer to a specified level.
CloseSharedFiles	Closes a shared file and removes the file lock.
DeleteGroup	Deletes a local or domain Windows group account.
DeleteUser	Deletes a local or domain Windows user account.
FileCheck	Checks whether a particular file exists.
ModifyServiceConfig	Changes the configuration for specified services.
RegistrySet	Sets or creates a Windows registry key.
RestartService	Schedules a service to automatically stop and restart a service after a specified time interval.
RunDOS	Runs a non-interactive DOS command.
SNMPSet	Sets a value for a selected SNMP MIB variable.
SyncTime	Synchronizes the system time among computers.

Knowledge Script	What It Does
UnixAgentHealthProxy	Checks the availability of a remote managed UNIX computer and monitors the health of the remote UNIX agent. This Knowledge Script uses a proxy Windows agent to monitor remote UNIX agents.

AddGroup

Use this Knowledge Script to add a Windows domain group account or local group account. Domain groups are added to the domain associated with the managed computer where the script runs. This script raises an event when the operation is successful or when it fails.

Note
You cannot create a local group on a Windows Domain Controller.

Prerequisite

Before running this script, ensure the NetIQ Corporation AppManager Client Resource Monitor service (`netiqmc.exe`) is set to log on as a domain user account in the same domain as, or a domain trusted by, the target computer.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Name of group to be added	Provide the name of the domain group account to add. If you enter a group name for a Windows 2000 server domain controller exceeding the limit Active Directory can display in the **Name** column, the group name is displayed as S-1-5-21-952230801-75384649-2348082356-1114. To view the true group name and to verify that the group was created correctly, select **Users** in Active Directory Users and Computers and double-click the group name in the **Name** column. Active Directory Users and Computers displays the group name in **Group name (pre-Windows 2000)**.
Event if group was added?	Set to **y** to raise an event if the domain group was added. The default is n.
Event if group was not added?	Set to **y** to raise an event if the domain group was not added. The default is y.
Add local group?	Set to **y** to create a local group account on the computer where the script job is running. If set to n, you must enable *Add domain group?* to add a domain group. The default is n.
Add domain group?	Set to **y** to associate the domain group account with the domain of the computer where the script job is running. If set to n, you must enable *Add local group?* to add a local group. The default is y.

Parameter	How to Set It
Event severity: Group was not added	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a domain group was not added. The default is 12 (yellow event indicator).
Event severity: Group was added	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a domain group was added. The default is 25 (blue event indicator).

AddGroupViaAD

Use this Knowledge Script to add a domain group account to Active Directory. You must run this script on a computer that is a Domain Controller. The group is added to the domain associated with the managed computer where the script runs. This script raises an event when the operation is successful or when it fails.

Prerequisite

Before running this script, ensure the NetIQ Corporation AppManager Client Resource Monitor (`NetIQmc.exe`) service is set to log on as a domain user account in the same domain as, or a domain trusted by, the target computer.

Resource Objects

For AppManager version 7.x: Domain Controller computers running Windows 2000 Server, Windows Server 2003, or Windows Server 2008

For AppManager version 6.x: Domain Controller computers running Windows 2000 Server or Windows Server 2003

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Name of group to be added	Provide the name of the domain group account to add. If you enter a group name for a Windows 2000 server domain controller exceeding the limit Active Directory can display in the **Name** column, the group name is displayed as S-1-5-21-952230801-75384649-2348082356-1114. To view the true group name and verify that the group was created correctly, select **Users** in Active Directory Users and Computers and double-click the group name in the **Name** column. Active Directory Users and Computers displays the group name in **Group name (pre-Windows 2000)**.
Event if group was added?	Set to **y** to raise an event if the domain group was added. The default is n.
Event if group was not added?	Set to **y** to raise an event if the domain group was not added. The default is y.
Event severity: Group was not added	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a domain group was not added. The default is 12 (yellow event indicator).
Event severity: Group was added	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a domain group was added. The default is 25 (blue event indicator).

AddUser

Use this Knowledge Script to add a domain user account or local user account. A domain user account is added to the domain associated with the managed computer where the script runs. This script raises an event when the operation succeeds or fails.

Note
You cannot create a local user on a Windows Domain Controller.

Prerequisite

Before running this script, ensure the NetIQ Corporation AppManager Client Resource Monitor service (`NetIQmc.exe`) is set to log on as a domain user account in the same domain as, or a domain trusted by, the target computer.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Name of user to be added	Provide the name of the user account to add.
Password of user to be added	Provide the password of the user account to add.
Event if user was added?	Set to **y** to raise an event if the user was added. The default is n.
Event if user was not added?	Set to **y** to raise an event if the user was not added. The default is y.
Add domain user?	Set to **y** to add the user as a domain user in the current client's domain. If set to y, the user account is associated with the domain of the computer where the script is running. If set to n, a local user account is created on the computer where the script is running. The default is y.
Event severity: User was not added	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the user was not added. The default is 12 (yellow event indicator).
Event severity: User was added	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the user was added. The default is 25 (blue event indicator).

AddUserViaAD

Use this Knowledge Script to add a user account to Active Directory. You must run this script on a computer that is a Domain Controller. The user account is added to the domain associated with the computer where the script runs. This script raises an event when the operation is successful or when it fails.

Prerequisite

Before running this script, ensure the NetIQ Corporation AppManager Client Resource Monitor service, `NetIQmc.exe`, is set to log on as a domain user account in the same domain as, or a domain trusted by, the target computer.

Resource Objects

For AppManager version 7.x: Domain Controller computers running Windows 2000 Server, Windows Server 2003, or Windows Server 2008

For AppManager version 6.x: Domain Controller computers running Windows 2000 Server or Windows Server 2003

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Name of user to be added	Provide the name of the user account to add.
Password of user to be added	Provide the password of the user account to add.
Event if user was added?	Set to **y** to raise an event if the user account was added. The default is y.
Event if user was not added?	Set to **y** to raise an event if the user account was not added. The default is y.
Event severity: User was not added	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the user was not added. The default is 12 (yellow event indicator).
Event severity: User was added	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the user was added. The default is 25 (blue event indicator).

ChangePassword

Use this Knowledge Script to change the password for a specified domain user account or local user account. This script raises an event when the change password operation is successful or when it fails.

Prerequisite

Before running this script, ensure the NetIQ Corporation AppManager Client Resource Monitor service (`NetIQmc.exe`) is set to log on as a domain user account in the same domain as, or a domain trusted by, the target computer.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Name of user account	Provide the name of the user account whose password should be changed. The default is guest.
New password for user account	Provide the new password for the user account.
Is the account a domain user?	Set to **y** to change the password for a domain user account. Set to **n** to change the password for a local user account. If set to y, the affected domain user account is one associated with the domain of the managed client where the Knowledge Script job is running. The default is y.
Event if password was changed	Set to **y** to raise an event if the password is changed successfully. The default is n.
Event if password was not changed	Set to **y** to raise an event if the password is not changed. The default is y.
Event severity: Password was not changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the password was not changed. The default is 12 (yellow event indicator).
Event severity: Password was changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the password was changed. The default is 25 (blue event indicator).

CheckServicePack

Use this Knowledge Script to compare the installed version of a Microsoft Windows service pack to a specified minimum threshold. This script raises an event if the version of the service pack installed on the target computer falls below the minimum threshold.

This script queries the computer's registry to determine the current service pack level.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Weekly**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Create event if service pack does not meet minimum?	Select **Yes** to raise an event if the version of the service pack installed on the target computer falls below the threshold. The default is Yes.
Severity - Service pack does not meet minimum	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service pack version falls below the threshold. The default is 8 (red event indicator).
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the CheckServicePack job fails. The default is 8 (red event indicator).
Data Collection	
Collect service pack data?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the target computer's configuration, including the Windows version and service pack number. The default is unselected.
Monitoring	
Check Windows 2000 Service Pack?	Select **Yes** to check the Windows 2000 Service Pack level on the target computer. The default is Yes.
Threshold -- Service pack minimum	Specify the minimum version of the Windows 2000 service pack that must be installed to prevent an event from being raised. For example, to check whether Service Pack 4 (or later) is installed, enter 4. The default is 4.
Check Windows XP Service Pack?	Select **Yes** to check the Windows XP service pack level on the target computer. The default is Yes.
Threshold -- Service pack minimum	Specify the minimum version of the Windows XP service pack that must be installed to prevent an event from being raised. For example, to check whether Service Pack 1 (or later) is installed, enter 1. The default is 3.
Check Windows 2003 Service Pack?	Select **Yes** to check the Windows Server 2003 service pack level on the target computer. The default is Yes.

Parameter	How to Set It
Threshold - Service pack minimum	Specify the minimum version of the Windows Server 2003 service pack that must be installed to prevent an event from being raised. For example, to check whether Service Pack 1 (or later) is installed, enter 1. The default is 2.
Check Windows Vista Service Pack?	Select **Yes** to check the Windows Vista service pack level on the target computer. The default is Yes.
Threshold - Service pack minimum	Specify the minimum version of the Windows Vista service pack that must be installed to prevent an event from being raised. For example, to check whether Service Pack 1 (or later) is installed, enter 1. The default is 2.
Check Windows Server 2008 Service Pack?	Select **Yes** to check the Windows Server 2008 service pack level on the target computer. The default is Yes.
Threshold - Service pack minimum	Specify the minimum version of the Windows Server 2008 service pack that must be installed to prevent an event from being raised. For example, to check whether Service Pack 1 (or later) is installed, enter 1. The default is 2.
Check Windows 7 Service Pack?	Select **Yes** to check the Windows 7 service pack level on the target computer. The default is Yes.
Threshold - Service pack minimum	Specify the minimum version of the Windows 7 service pack that must be installed to prevent an event from being raised. For example, to check whether Service Pack 1 (or later) is installed, enter 1. The default is 0.
Check Windows Server 2008 R2 Service Pack?	Select **Yes** to check the Windows Server 2008 R2 service pack level on the target computer. The default is Yes.
Threshold - Service pack minimum	Specify the minimum version of the Windows Server 2008 R2 service pack that must be installed to prevent an event from being raised. For example, to check whether Service Pack 1 (or later) is installed, enter 1. The default is 0.

CloseSharedFiles

Use this Knowledge Script to close one or more shared files and remove corresponding file locks. You must run this script on the server where the file is shared.

You must specify a shared file by its file identifier. You can view the file identifier in one of the following ways:

- At a Command Prompt, run the `net file` command to see a list of files, corresponding identifiers, and lock information.
- See the SharedFiles Knowledge Script.

Prerequisite

Before running this script, ensure the NetIQ Corporation AppManager Client Resource Monitor service (`NetIQmc.exe`) is set to log on as a domain user account in the same domain as, or a domain trusted by, the target computer.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
List of file identifiers	Specify the file identifier for each file you want to close. Use a comma to separate multiple identifiers. The default is 1,2,3.
Event if file was closed?	Set to **y** to raise an event if the file is closed successfully. The default is n.
Event if file was not closed?	Set to **y** to raise an event if the file is not closed. The default is y.
Event severity: File was not closed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the file was not closed. The default is 12 (yellow event indicator).
Event severity: File was closed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the file was closed. The default is 25 (blue event indicator).

DeleteGroup

Use this Knowledge Script to delete a specified domain group account or local group account. This script raises an event when the group is deleted successfully or when the deletion fails.

Prerequisite

Before running this script, ensure the NetIQ AppManager Client Resource Monitor service, `NetIQmc.exe`, is set to log on as a domain user account in the same domain as, or a domain trusted by the target computer.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Name of the group to be deleted	Provide the name of the group account you want to delete.
Event if group is deleted?	Set to **y** to raise an event if the group account is deleted successfully. The default is n.
Event if group is not deleted?	Set to **y** to raise an event if the group account is not deleted. The default is y.
Delete local group?	Set to **y** to delete a local group. If set to n, you must enable *Delete domain group?* to delete a domain group. The default is n.
Delete domain group?	Set to **y** to delete a domain group account. If set to n, enable *Delete local group?* to delete a local group. If set to y, the domain account affected is one associated with the domain of the computer where the job is running. The default is y.
Event severity: Group was not deleted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the group was not deleted. The default is 12 (yellow event indicator).
Event severity: Group was deleted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the group was deleted. The default is 25 (blue event indicator).

DeleteUser

Use this Knowledge Script to delete a specified domain user account or local user account. This script raises an event when the user account is deleted successfully or when the deletion fails.

Prerequisite

Before running this script, ensure theNetIQ Corporation AppManager Client Resource Monitor service (`NetIQmc.exe`) is set to log on as a domain user account in the same domain as, or a domain trusted by, the target computer.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Name of the user to be deleted	Provide the name of the user account you want to delete.
Event if user is deleted?	Set to **y** to raise an event if the user account is deleted successfully. The default is n.
Event if user is not deleted?	Set to **y** to raise an event if the user account is not deleted. The default is y.
Delete domain user?	Set to **y** to delete a domain user account. Set to **n** to delete a local user account. If set to n, the local user account affected is one associated with the domain of the computer where the script is running. The default is y.
Event severity: User was not deleted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the user was not deleted. The default is 12 (yellow event indicator).
Event severity: User was deleted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the user was deleted. The default is 25 (blue event indicator).

FileCheck

Use this Knowledge Script to check whether a particular file exists on one or more computers. This script raises an event if it finds the file you specified.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Full path to file	Provide the full path to the file you want to check, for example: `c:\winnt35\system32\clock.exe` **Notes** • If you include spaces in the filepath, the event details include a broken link to the file. • If the file is on a network-mounted drive, the computer where you run this script must be running with a Windows domain account that can access the remote drive. Otherwise, the job may report an error because it cannot access files on the remote drive.
Event when found?	Set to **y** to raise an event if the specified file is found. If set to n, an event is raised when the file cannot be found. The default is y.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the specified file is found or not found. The default is 5 (red event indicator).

ModifyServiceConfig

Use this Knowledge Script to change the configuration for specified services. To apply your changes, you must manually restart the services. This script raises an event indicating whether the service configuration change you specified was successful.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
List of services	Provide the names of the services whose configurations you want to modify, separating the names with commas (,). Enter the internal service names or the service names displayed in the Services Control Panel.
Collect data?	Set to **y** to collect data. If enabled, data collection returns: • **100** -- service successfully modified, or • **0** -- service modification failed. The default is n.
Service type	Select a new service type. Valid types are: • own • share • interact • kernel • filesys Select `NO_CHANGE` to keep the current configuration. Default is `NO_CHANGE`.
Start type	Select a new start type. Valid types are: • boot • system • auto • demand • disabled Select `NO_CHANGE` to keep the current configuration. Default is `NO_CHANGE`.

Parameter	How to Set It
Error control	Select the level of error control. Valid types are: • normal • severe • critical • ignore Select NO_CHANGE to keep the current configuration. Default is NO_CHANGE.
Log On As account	Specify the system or user account name for the service to log on as. Although most services log on as a system account, you can configure some services to log on using special user accounts. Default is NO_CHANGE. **Note** The account you specify here must already have the right to log on as a service.
Password for Log On As account	Specify the password for the logon user account.
Display name of the service	Provide a new display name for the service. The default is NO_CHANGE.
Event severity: Service was changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service was changed. The default is 20 (yellow event indicator).
Event severity: Service was not changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service was not changed. The default is 8 (red event indicator).

RegistrySet

Use this Knowledge Script to set or create a Windows registry key. You can specify a list of computers where you want to set the key value, either directly using the *List of computers* parameter or in a file containing a list of computer names or addresses. This script creates a new key if the specified key does not exist. In addition, this script raises an event if the set operation fails. This script can also raise an event if the set operation completes successfully.

On 64-bit Windows systems, you can configure this script to set registry information for 32-bit or 64-bit programs.

- To set registry information for a 64-bit application, disable the *Set 32-bit program registry keys on a 64-bit system?* parameter and specify the registry path and key under `HKEY_LOCAL_MACHINE\Software`.
- To set registry information for a 32-bit application, enable the *Set 32-bit program registry keys on a 64-bit system?* parameter and specify the registry path and key exactly as it would be specified on a 32-bit system, under `HKEY_LOCAL_MACHINE\Software`.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event when set?	Set to **y** to raise an event when the registry key is set successfully. The default is n.
Set 32-bit program registry keys on a 64-bit system?	On a 64-bit Windows system, set this parameter to **y** to set registry information for 32-bit programs. The default value, n, enables you to set registry information for 64-bit programs. On a 32-bit Windows system, this parameter is not applicable and will be ignored. **Tip** To set registry information for 32-bit programs and 64-bit programs, configure separate jobs.
Root key	Specify the registry root. Valid root options are: • `HKEY_LOCAL_MACHINE` • `HKEY_CLASSES_ROOT` • `HKEY_CURRENT_USER` • `HKEY_USERS` The default is `HKEY_LOCAL_MACHINE`.

Parameter	How to Set It
Full path to registry key	Provide the full path to the registry key. You can enter any path under the root key as long as you have write permission. The default path is: `Software\NetIQ\AppManager\4.0\NetIQmc\Tracing` To specify the path to the registry key for a 32-bit or 64-bit program, specify a path under `HKEY_LOCAL_MACHINE\Software`. **Note** Although the registry keys for 32-bit programs on a 64-bit system are stored under the key `HKEY_LOCAL_MACHINE\Software\Wow6432Node`, **do not** specify the `Wow6432Node` component of the path. Instead, specify the path without the `Wow6432Node` component, and enable the *Set 32-bit program registry keys on a 64-bit system?* parameter.
Key name	Specify the name of the key to set or create. The default is `TraceMC`.
Key type	Specify the type for the key. Valid types are: • `REG_SZ` • `REG_MULTI_SZ` • `REG_DWORD` • `REG_EXPAND_SZ` The default is `REG_DWORD`.
Value of the key	Specify the value to which the registry key should be set. Hex values can be entered in the form 0x*nnnn*. Default is 1.
Null character	Specify the character separator for `REG_MULTI_SZ` type. For example to set *foo bar*, you need to be able to indicate the blank space between *foo* and *bar* (foo+bar). The default is +. **Note** Choose a character that is not part of the name.
List of computers (comma separated)	Specify the computers for which you want to set this value. If you leave this parameter blank, the registry key located on the local computer is set. To set the value for multiple computers, enter the hostname or IP address for each computer in a comma-separated list. For example: `CORP01,ENGR02,10.15.221.5.`

Full path to file with list of computers	To set values for more computers than is convenient to enter one at a time in the *List of computers* parameter, create a file that contains a list of the computers you want to monitor.
	Provide the full path to the file containing a list of the computers whose registry key values you want to set. The file should contain the hostname or IP address for each computer in one or more lines. Each line can have multiple computer names, separated by commas. For example:
	`NYC01,NYC02`
	`SALES01,10.15.221.5,SFO01`
	`LABMACH, QATEST`

Severity: Key was set	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the key is set. The default is 16 (yellow event indicator).
Severity: Key was not set	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the key is not set. The default is 5 (red event indicator).

RestartService

Use this Knowledge Script to schedule a service to automatically stop and restart after a specified interval. You can also have the script restart any services that depend on the ones you have stopped. This script raises an event if it fails to restart a service. Note that you cannot use this script to stop the NetIQ Client Resource Monitor (`netiqmc`) agent service.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Daily**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Create event if service restarts successfully?	Select **Yes** to raise an event if the script successfully restarts a service and, optionally, its dependent services. The default is Yes.
Severity - Service restarted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the script successfully restarts a service. The default is 25 (blue event indicator).
Create event if service restart fails?	Select **Yes** to raise an event if the script fails to restart a service. The default is Yes.
Severity - Service start failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the script fails to restart a service. The default is 5 (red event indicator).
Severity - Service stop failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the script fails to stop a service. The default is 5 (red event indicator).
Create event if service is missing?	Select **Yes** to raise an event if a specified service is missing. The default is unselected.
Severity - Service missing	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a specified service is missing. The default is 8.
Create event if service is disabled?	Select **Yes** to raise an event if the script disables a service. The default is Yes.
Severity - Service disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the script disables a service. The default is 12.
Create event if service is shut down normally? (5.0+)	Select **Yes** to raise an event if the script shuts down a service normally. The default is Yes. **Note** An event is raised if a service is shut down normally only by AppManager agents version 5.0 and later.

Parameter	How to Set It
Severity - Service shut down normally	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the script shuts down a service normally. The default is 30.
Severity - Job Failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the RestartService job fails unexpectedly. The default is 10 (red event indicator).
Data Collection	
Collect data?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: • **100** -- service was restarted successfully, or • **0** -- service did not restart. The default is unselected.
Administration	
Service list	Provide the names of the services to you want to stop. Separate each name with a comma (,) and no spaces. The default is `Alerter,Messenger`.
Service start/stop delay	Specify the number of seconds to wait after a service is stopped before attempting to automatically restart it. The default is 30.
Restart dependent services? (6.0+)	Select **Yes** to also restart any services that depend on the services you stopped. The default is Yes. For example, if you stop the `MSSQLSERVER` service, the `SQLSERVERAGENT` service is also stopped. You can use this parameter to restart the agent service along with the server. **Note** Dependent services are restarted only by AppManager agents version 6.0 and later.
Service start/stop retry count	Specify the number of times to attempt to restart a service after it has stopped. The default is 3 times.
Restart service if shut down normally? (5.0+)	Select **Yes** to restart a service that is shut down normally. By default, this script restarts services that are shut down normally. **Note** A service that is shut down normally is restarted only by AppManager agents version 5.0 and later.

RunDOS

Use this Knowledge Script to run a non-interactive DOS command. This script raises an event if an unexpected exit code is raised. For example, use this script to run a batch command for virus scanning, disk backup, or logging an entry in a trouble ticket system.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Create event if command executes successfully?	Select **Yes** to raise an event if the DOS command you specified executes successfully. The default is unselected.
Severity - Command executed successfully	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the specified DOS command executes successfully. The default is 25 (blue event indicator).
Create event if process failed to execute?	Select **Yes** to raise an event if the DOS command you specified did not execute successfully. The default is Yes.
Severity - Command failed to execute	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the specified DOS command did not execute successfully. The default is 5 (red event indicator).
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the RunDOS job fails unexpectedly. The default is 5 (red event indicator).
Data Collection	
Collect exit code data?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns exit code data; including the specified command string, current exit code, normal exit code, and explanation. The default is unselected.
Administration	
Normal/Expected exit code	Specify the exit (return) code expected when the command runs and exits normally (successfully). The default is 0.
Command or full path to script file	Specify the DOS command or script filename to run. For example, `C:\temp\myscript.bat`. Do not use a command that requires input. **Note** If the command you are entering includes quotation marks ("), enclose the quoted string in a second set of quotation marks. For example, if the DOS command is `net send "message"` you would enter: `net send ""message""`.

Parameter	How to Set It
Full path to command output file	Provide the full path and filename to specify a file to write command output. If you do not specify the full path, AppManager creates the file in `WINNT\System32\`.
Full path to error output file	Provide the full path and filename to specify a file to write error output. If you do not specify the full path, AppManager creates the file in `WINNT\System32\`.
Append to output files?	Select **Yes** to add information to the command and error output files. The default is Yes.
Time to wait for process to complete	Specify the maximum number of seconds the specified DOS command or script file should take to execute. The default is 10. Set to 0 to run the DOS command without checking the exit code.

SNMPSet

Use this Knowledge Script to perform an SNMP v1 `Set` operation for the selected SNMP MIB variable. You can specify a list of computers where you want to set the variable value directly using the *List of computers* parameter or in a file containing a list of computer names or addresses. This script raises an event if the `Set` operation encounters an error and, optionally, if the `Set` operation completes successfully. This script requires the Microsoft SNMP Service to be running and security for the service set to allow Read and Write privileges.

Prerequisite

By default, the security for the Microsoft SNMP Service is typically set to the read-only permission level. To use this script, the Microsoft SNMP Service must be set to the read/write permission level. For more information, see the following topics:

- "Checking SNMP Service Rights" on page 3214
- "Changing the Permission Level for the SNMP Service" on page 3215

Resource Objects

Windows server or HP SIM server

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the `Set` operation completes successfully. The default is n. This script always raises an event if the `Set` operation encounters an error.
Object identifier	For the MIB variable, specify the MIB object identifier in the OID notation (for example `.1.2.3.456.78`) or ODE notation (for example, `system.sysUptime.0`). The default is `system.sysContact.0`. If you are using the object identifier (OID), you must include the dot (.) at the beginning of the identifier. If you are using the object descriptor (ODE), use a case-sensitive descriptor. You can use the object descriptor if the `mib.bin` file has been compiled on the agent machine (in the `%windir%/system32` directory). For information about compiling the `mib.bin`, see the Windows Resource Kit.
Community string	Provide a valid SNMP community string name. Leave this parameter blank to use the SNMP community name entered in AppManager Security Manager. The default is public.

Parameter	How to Set It
Set type	Specify the data type for the MIB variable to set. Valid values are: • OCTETSTRING • INTEGER • COUNTER • GAUGE • TIMETICKS • IPADDRESS The default is OCTETSTRING.
Set value	Specify the value you want to set.
List of computers	Specify the computers whose values you want to set. If you leave this parameter blank, this script sets the SNMP MIB variable located on the managed computer where the Knowledge Script job is running. To set the value for multiple computers, enter the hostname or IP address for each computer in a comma-separated list. For example: CORP01,ENGR02,10.15.221.5
Full path to computer list file	To set values on more computers than is convenient to list one at a time in the *List of computers* parameter, create a file containing a list of the computers whose values you want to set. Enter the full path to the file. The file should contain the hostname or IP address for each computer in one or more lines. Each line can have multiple computer names, separated by commas. For example: NYC01,NYC02 SALES01,10.15.221.5,SFO01 LABMACH, QATEST
Event severity: Variable was not set	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the specified value was not set. The default is 5 (red event indicator). This script always raises an event when a Set operation fails.
Event severity: Variable was set	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the variable was set. Default is 16 (yellow event indicator). The *Event?* parameter must be enabled to raise an event for a successful Set operation.
Threshold for attempts to contact SNMP agent	Specify the maximum number of times the script should try to contact the SNMP agent before raising an event. The default is 3 times.
Threshold (in seconds) for a response	Specify the maximum number of seconds the script should wait for a response from the SNMP agent before timing out and raising an event. The default is 5 seconds.

Checking SNMP Service Rights

By default, the Microsoft SNMP Service is typically configured with Read-only permission. This configuration will prevent the SNMPSet Knowledge Script from setting any values. You can check your current configuration for any computer using the Services Control Panel.

To check the rights associated with the Microsoft SNMP Service:

1. In the Services Control Panel, select the Microsoft SNMP Service, and then click the **Security** tab.
2. Verify the rights associated with the community name you are using for the computer are READ WRITE.

Changing the Permission Level for the SNMP Service

To change the rights associated with the Microsoft SNMP Service:

1. In the Services Control Panel, select the Microsoft SNMP Service, and then click the **Security** tab.
2. Select the community name you are using, then click **Edit**.
3. Select the `READ WRITE` permission level from the Community rights list.
4. Click **OK**.

SyncTime

Use this Knowledge Script to synchronize the system time among computers. This script uses the Windows `net time` command to synchronize the system time to a specified Windows computer, such as the Primary Domain Controller in a workgroup. If you do not specify a computer name, the Domain Controller for the local computer is used. This script raises an event if the time synchronization operation fails.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default schedule for this script is **Daily**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the time synchronization operation fails. The default is y.
Name of computer with standard time	Specify the name of the computer whose system time you want the target computers synchronized to match. If you do not specify a computer name, this script uses the Domain Controller associated with the managed computer on which the script is running.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the time synchronization operation fails. The default is 12 (yellow event indicator).

UnixAgentHealthProxy

Run this Knowledge Script on a proxy Windows agent to remotely monitor the health of UNIX agents. This script performs the following tasks:

- Checks the availability of a managed UNIX computer by first sending an ICMP Echo request to the managed UNIX computer. If the remote computer does not respond, this script sends an ICMP Echo request to the managed UNIX computer's default router and raises an event.
- Monitors the health of the UNIX agent by checking a time stamp value created by the UNIX agent. Normally, the UNIX agent creates a time stamp value every 90 seconds. If the age of the time stamp value exceeds the threshold, this script raises an event and restarts the UNIX agent.

Use this script to validate the health of the UNIX agent on a scheduled basis or for diagnostic purposes (for example, if there are gaps in data collection). This script can detect a problem with a remote agent and reliably notify the AppManager administrator.

The remote UNIX computer to be monitored must be accessible through the network from the computer where the proxy Windows agent is installed. To use this script to monitor more than one remote managed UNIX computer, all the computers you want must be accessible using the same **root** user account information.

Note

If you specify an incorrect password for the root account when running this script with Secure Shell (SSH) as the connection method to the remote UNIX or Linux computer, the script raises an event that incorrectly states that the login attempt was successful. If you see an event message similar to the event message below, you must update the job properties to specify the correct root password and start the job:

```
Output: Permission denied at /usr/netiq/UnixAgent/bin/UnixAgentHealthProxy.pl
More Info: "SSH login OK to <machine> with root Using SSH/SFTP combination."
```

Resource Objects

A managed UNIX computer where the AppManager UNIX agent is installed. The UNIX agent must be configured to run as the root user account.

Default Schedule

The default interval for this script is **Every 10 minutes**.

To avoid raising false events, do not configure this script to run more frequently than the UNIX agent updates its time stamp. Ideally, the interval should be more than four minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event if age of timestamp exceeds threshold?	Set to **y** to raise an event if the age of the time stamp exceeds the threshold you set. The default is y.
Threshold – Maximum age of timestamp	Specify the maximum age a time stamp can attain before an event is raised. The minimum threshold is 3 minutes and the maximum threshold is 99999 minutes. The default is 9 minutes.

Parameter	How to Set It
Event severity when age of timestamp exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the age of the time stamp exceeds the threshold. The default is 8.
Remote Host Connection	
UNIX computers to monitor (comma-separated)	Specify the IP addresses of the remote UNIX computers you want to monitor, separating the addresses with commas and no spaces.
Password for root user account	Specify the root user account password that the proxy agent computer must use to connect to the remote UNIX computer. This is a mandatory field.
Connection Transport	Specify the connection mode between the proxy agent computer and the monitored UNIX computer: • **Telnet/FTP** to connect using Telnet. • **SSH/FTP** to connect using SSH. This script can use either the Secure Shell (SSH) program with root password authentication or Telnet to make a secure connection to the remote UNIX or Linux computer. If you choose to use Telnet, you must supply a non-root user account name and password. **Note** Telnet and FTP send your user name, password, and other information across the network in cleartext, making it easy for others to read this data.
Telnet non-root user account	Provide the Telnet non-root user account if you are using Telnet to connect to the monitored UNIX computer. Leave this parameter value blank if you are using SSH to connect to the monitored UNIX computer.
Telnet non-root user password	Provide the Telnet non-root user password if you are using Telnet to connect to the monitored UNIX computer. Leave this parameter value blank if you are using SSH to connect to the monitored UNIX computer.
Restart UNIX agent if age of timestamp exceeds threshold?	Set to **y** to restart the UNIX agent if the age of the time stamp exceeds the threshold you set. The default is y.

Chapter 55
OCS Knowledge Scripts

Microsoft OCS combines enterprise-ready instant messaging, presence capabilities, conferencing, unified communications, and administrative controls in a single offering. OCS adds real-time conferencing hosted on servers inside the corporate firewall to existing features such as federation and public instant-messaging connectivity.

AppManager for Microsoft OCS provides the following Knowledge Scripts for monitoring Microsoft OCS resources. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ArchivedVoIPCallActivity	Monitors the various VoIP call metrics contained in the Monitoring database.
ConferenceCallActivity	Monitors the number of active conferences and how many users are in those conferences.
CWAIMFailures	Monitors the current IM session failures on the CWA server.
CWAIMSessionActivity	Monitors the current IM sessions on the Communicator Web Access (CWA) server.
CWAServerStatus	Monitors the CWA server status for throttling states.
CWAUserSessionActivity	Monitors the current user sessions on the CWA server.
CWAUserSessionFailures	Monitors the current session failures on the CWA server.
EdgeServerCallActivity	Monitors current call activity metrics for the Edge server.
EdgeServerCallFailures	Monitors current call failure metrics for the Edge server.
HealthCheck	Monitors the running status of primary services of the OCS server.
MCUStatus	Monitors the status of various services installed on the OCS server.
MediationServerCallActivity	Monitors inbound and outbound call activities on the Mediation server.
MediationServerCallFailures	Monitors the MediaRelay engine components of the Mediation server.
MediationServerHealth	Monitors server health metrics for the Mediation server.
MediationServerUsage	Monitors server resource usage for the Mediation server.
SessionCallActivity	Monitors data about the number of current sessions.
SessionCallFailures	Queries the Call Detail Record server to find any known session failures.
SystemUptime	Monitors the length of time a system has been up and running since a reboot.
SystemUsage	Monitors the total CPU usage of the server using OCS.

ArchivedVoIPCallActivity

Use this Knowledge Script to monitor the various Voice over IP (VoIP) call metrics contained in the Monitoring database. This script monitors the number of total VoIP calls made, the types of calls made, the average duration of calls, the number of redirected calls, and the number of calls per gateway.

A **gateway** is third-party hardware that connects Microsoft OCS with a public switched telephone network (PSTN), private branch exchange (PBX), or other phone system.

Resource Objects

OCS_ArchivingandCDRFolder

OCS_CDRObject

Default Schedule

The default interval for this script is **15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Total Number of VoIP Calls	
Event Notification	
Raise event if total number of VoIP calls exceeds the threshold?	Set to **Yes** to raise an event if the number of VoIP calls exceeds the threshold. The default is Yes.
Threshold - Maximum total number of VoIP calls	Specify the maximum number of VoIP calls that can be active before an event is raised. The default is 20.
Event severity when total number of VoIP calls exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of VoIP calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for total number of VoIP calls?	Set to **Yes** to collect data about the number of VoIP calls. The default is Yes.
Monitor Total Number of UC to PSTN Calls	
Event Notification	
Raise event if total number of UC to PSTN calls exceeds threshold?	Set to **Yes** to raise an event if the number of unified communications (UC) calls to public switched telephone network (PSTN) calls exceeds the threshold. The default is Yes.
Threshold - Maximum total number of UC to PSTN calls	Specify the maximum number of UC to PSTN calls that can be active before an event is raised. The default is 20.

Description	How to Set It
Event severity when total number of UC to PSTN calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for total number of UC to PSTN calls?	Set to **Yes** to collect data about the number of UC to PSTN calls. The default is Yes.
Monitor Total Number of PSTN to UC Calls	
Event Notification	
Raise event if total number of PSTN to UC calls exceeds threshold?	Set to **Yes** to raise an event if the number of PSTN to UC calls exceeds the threshold. The default is Yes.
Threshold - Maximum total number of PSTN to UC calls	Specify the maximum number of PSTN to UC calls that can be active before an event is raised. The default is 20.
Event severity when total number of PSTN to UC calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for total number of PSTN to UC calls?	Set to **Yes** to collect data about the number of PSTN to UC calls. The default is Yes.
Monitor Average Duration of Calls	
Event Notification	
Raise event if average duration of calls exceeds threshold?	Set to **Yes** to raise an event if the average duration of calls exceeds the threshold. The default is Yes.
Threshold - Maximum average duration of calls	Specify the maximum average call duration that can occur before an event is raised. The default is 20.
Event severity when the average duration of calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the average duration of calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for average duration of calls?	Set to **Yes** to collect data about the average duration of calls. The default is Yes.
Monitor Number of Redirected Calls	
Event Notification	
Raise event if total number of redirected calls exceeds threshold?	Set to **Yes** to raise an event if the number of **redirected**, or transferred, calls exceeds the threshold. The default is Yes.
Threshold - Maximum total number of redirected calls	Specify the maximum number of calls that can be redirected before an event is raised. The default is 20.
Event severity when total number of redirected calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of redirected calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of redirected calls?	Set to **Yes** to collect data about the number of redirected calls. The default is Yes.
Monitor Number of Calls per Gateway	

Description	How to Set It
Event Notification	
Raise event if total number of calls per gateway exceeds threshold?	Set to Yes to raise an event if the number of calls per gateway exceeds the threshold. The default is Yes.
Threshold - Maximum total number of calls per gateway	Specify the maximum number of calls that the gateway can handle before an event is raised. The default is 20.
Event severity when total number of calls per gateway exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of calls per gateway?	Set to **Yes** to collect data about the number of calls per gateway. The default is Yes.

ConferenceCallActivity

Use this Knowledge Script to monitor the number of active conferences, and the number of users involved in those conferences, on an OCS server. The conference type can be instant message (IM), telephony, A/V, or Web.

Resource Object

OCS_ConferenceObject

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor IM Conferences	
Event Notification	
Raise event if number of IM conferences exceeds threshold?	Set to **Yes** to raise an event if the number of instant message conferences exceeds the threshold. The default is Yes.
Threshold - Maximum IM conferences	Specify the maximum number of IM conferences that can be active before an event is raised. The default is 25.
Event severity when number of IM conferences exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of IM conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for IM conferences?	Set to **Yes** to collect data about the number of IM conferences. The default is No.
Monitor A/V Conferences	
Event Notification	
Raise event if number of A/V conferences exceeds threshold?	Set to **Yes** to raise an event if the number of A/V conferences exceeds the threshold. The default is Yes.
Threshold - Maximum A/V conferences	Specify the maximum number of A/V conferences that can be active before an event is raised. The default is 25.
Event severity when number of A/V conferences exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of A/V conferences exceeds the threshold. The default is 15.
Data Collection	

Description	How to Set It
Collect data for A/V conferences?	Set to **Yes** to collect data about the number of A/V conferences. The default is No.
Monitor Telephony Conferences	
Event Notification	
Raise event if number of telephony conferences exceeds threshold?	Set to **Yes** to raise an event if the number of telephony conferences exceeds the threshold. The default is Yes.
Threshold - Maximum telephony conferences	Specify the maximum number of telephony conferences that can be active before an event is raised. The default is 25.
Event severity when number of telephony conferences exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of telephony conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for telephony conferences?	Set to **Yes** to collect data about the number of telephony conferences. The default is Yes.
Monitor Web Conferences	
Event Notification	
Raise event if number of Web conferences exceeds threshold?	Set to **Yes** to raise an event if the number of Web conferences exceeds the threshold. The default is Yes.
Threshold - Maximum Web conferences	Specify the maximum number of Web conferences that can be active before an event is raised. The default is 25.
Event severity when number of Web conferences exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of Web conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for Web conferences?	Set to **Yes** to collect data about the number of Web conferences. The default is Yes.
Monitor IM Conference Users	
Event Notification	
Raise event if number of IM conference users exceeds threshold?	Set to **Yes** to raise an event if the number of IM conference users exceeds the threshold. The default is Yes.
Threshold - Maximum number of IM conference users	Specify the maximum number of IM conference users that can be active before an event is raised. The default is 10.
Event severity when number of IM conference users exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of IM conference users exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of IM conference users?	Set to **Yes** to collect data about the number of IM conference users. The default is Yes.
Monitor A/V Conference Users	
Event Notification	
Raise event if number of A/V conference users exceeds threshold?	Set to **Yes** to raise an event if the number of A/V conference users exceeds the threshold. The default is Yes.

Description	How to Set It
Threshold - Maximum number of A/V conference users	Specify the maximum number of A/V conference users that can be active before an event is raised. The default is 10.
Event severity when number of A/V conference users exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of A/V conference users exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of A/V conference users?	Set to **Yes** to collect data about the number of A/V conference users. The default is Yes.
Monitor Telephony Conference Users	
Event Notification	
Raise event if number of telephony conference users exceeds threshold?	Set to **Yes** to raise an event if the number of telephony conference users exceeds the threshold. The default is Yes.
Threshold - Maximum number of telephony conference users	Specify the maximum number of telephony conference users that can be active before an event is raised. The default is 10.
Event severity when number of telephony conference users exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of telephony conference users exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of telephony conference users?	Set to **Yes** to collect data about the number of telephony conference users. The default is Yes.
Monitor Web Conference Users	
Event Notification	
Raise event if number of Web conference users exceeds threshold?	Set to **Yes** to raise an event if the number of Web conference users exceeds the threshold. The default is Yes.
Threshold - Maximum number of Web conference users	Specify the maximum number of Web conference users that can be active before an event is raised. The default is 10.
Event severity when number of Web conference users exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of Web conference users exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of Web conference users?	Set to **Yes** to collect data about the number of Web conference users. The default is Yes.

CWAIMFailures

Use this Knowledge Script to monitor instant messaging (IM) failures on the Communicator Web Access (CWA) server.

This script raises an event if the number of user session failures for IM exceeds the specified threshold and generates a data stream for the number of IM session failures.

Resource Object

OCS_CWAServerObject

Default Schedule

The default interval for this script is 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor IM Failures	
Event Notification	
Raise event if the number of IM failures exceeds threshold?	Set to **Yes** to raise an event if the number of instant messages that failed to be delivered exceeds the threshold. The default is Yes.
Threshold - Maximum IM failures	Specify the maximum number of IM failures that can be active before an event is raised. The default is 25.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of IM failures exceeds the threshold. The default is 15.
Data Collection	
Collect data for IM failures?	Set to **Yes** to collect data about the number of IM failures. The default is Yes.

CWAIMSessionActivity

Use this Knowledge Script to monitor current user session activity for instant messaging (IM) on the Communicator Web Access (CWA) server.

This script raises an event if the number of active user sessions for IM exceeds the specified threshold and generates a data stream for the number of active user sessions.

Resource Object

OCS_CWAServerObject

Default Schedule

The default interval for this script is 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor IM Sessions	
Event Notification	
Raise event if the number of active IM sessions exceeds threshold?	Set to **Yes** to raise an event if the number of active IM sessions exceeds the threshold. The default is Yes.
Threshold - Maximum active IM user sessions	Specify the maximum number of IM sessions that can be active before an event is raised. The default is 100.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of IM user sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of IM sessions?	Set to **Yes** to collect data about the number of active IM sessions. The default is Yes.

CWAServerStatus

Use this Knowledge Script to monitor the throttling states of the Communicator Web Access (CWA) Server. **Throttling** is when the number of connections are slow as a result of being overloaded. You can turn the throttling feature on or off when you configure your OCS server.

This script generates an event if the health state of a CWA server is throttling due to low available memory, high system CPU usage, or both.

Resource Object

OCS_CWAServerObject

Default Schedule

The default interval for this script is 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor CWA Server Throttling States	
Raise event if throttling is off?	Set to **Yes** to raise an event if the server throttling feature is off. The default is Yes. **Note**: The event for when server throttling is off is only raised on the first iteration of this script.
Event severity when throttling is off	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when throttling is off. The default is 20.
Raise event if throttling due to low available memory?	Set to **Yes** to raise an event if the cause of the server throttling is due to low available memory. The default is Yes.
Event severity when throttling due to low available memory	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the throttling state is low available memory. The default is 10.
Raise event if throttling due to high CPU usage?	Set to **Yes** to raise an event if the cause of the server throttling state is due to high CPU usage. The default is Yes.
Event severity when throttling due to high CPU usage	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the throttling state is high CPU usage. The default is 10.
Raise event if throttling due to low available memory and high CPU usage?	Set to **Yes** to raise an event when the cause of the server throttling is due to both low available memory and high CPU usage. The default is Yes.
Event severity when throttling due to low available memory and high CPU usage	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the throttling state is low available memory and high CPU usage. The default is 5.

CWAUserSessionActivity

Use this Knowledge Script to monitor the current user sessions on a Communicator Web Access (CWA) server.

This script raises an event if the number of active user session exceeds the specified threshold and generates a data stream for the number of active user sessions.

Resource Object

OCS_CWAServerObject

Default Schedule

The default interval for this script is 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor User Session Activity	
Event Notification	
Raise event if the number of active user sessions exceeds threshold?	Set to **Yes** to raise an event if the total number of active user sessions on the CWA server exceeds the threshold. The default is Yes.
Threshold - Maximum active user sessions	Specify the maximum number of active user sessions that can be active before an event is raised. The default is 100.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of active user sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for active user sessions?	Set to **Yes** to collect data about the number of active user sessions. The default is Yes.

CWAUserSessionFailures

Use this Knowledge Script to monitor the current user session failures on the Communicator Web Access (CWA) server.

This script raises an event if the number of user session failures exceeds the specified threshold and generates a data stream for the number of user session failures.

Resource Object

OCS_CWAServerObject

Default Schedule

The default interval for this script is 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor User Session Failures	
Event Notification	
Raise event if the number of user session failures exceeds threshold?	Set to **Yes** to raise an event if the number of user session failures exceeds the threshold. The default is Yes.
Threshold - Maximum user session failures	Specify the maximum number of user session failures that can be active before an event is raised. The default is 25.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of user session failures exceeds the threshold. The default is 15.
Data Collection	
Collect data for user session failures?	Set to **Yes** to collect data about the number of user session failures. The default is Yes.

EdgeServerCallActivity

Use this Knowledge Script to monitor call activity metrics for an Edge Server, including the number of active server connections. Also monitors the number of connections that are slow as a result of being overloaded, also known as **throttling**. This script also monitors the number of disconnected server connections.

Resource Object

OCS_EdgeServerFolder

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Active Server Connections	
Event Notification	
Raise event if the number of active server connections exceeds threshold?	Set to **Yes** to raise an event if the number of active server connections exceeds the threshold. The default is Yes.
Threshold - Maximum active server connections	Specify the maximum number of active server connections that can occur before an event is raised. The default is 100.
Event severity when the number of active server connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of active server connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for active server connections?	Set to **Yes** to collect data about the active server connections. The default is Yes.
Monitor Throttled Connections	
Event Notification	
Raise event if number of throttled connections exceeds threshold?	Set to **Yes** to raise an event if the number of throttled connections exceeds the threshold. Throttled connections are when connections are slow as a result of being overloaded. The default is Yes.
Threshold - Maximum throttled connections	Specify the maximum number of throttled connections that can occur before an event is raised. The default is 15.

Description	How to Set It
Event severity when the number of throttled connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of throttled connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for throttled connections?	Set to **Yes** to collect data about throttled connections. The default is Yes.
Monitor Disconnected Connections	
Event Notification	
Raise event if number of disconnected server connections exceeds threshold?	Set to **Yes** to raise an event if the number of disconnected server connections exceeds the threshold. The default is Yes.
Threshold - Maximum number of disconnected server connections	Specify the maximum number of disconnected server connections that can occur before an event is raised. The default is 25.
Event severity when the number of disconnected server connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of disconnected server connections exceeds the threshold. The default is 15.
Data Collection	
Collect data for disconnected server connections?	Set to **Yes** to collect data about disconnected server connections. The default is Yes.

EdgeServerCallFailures

Use this Knowledge Script to monitor current call failure metrics for an Edge server.

Resource Object

OCS_EdgeServerFolder

Default Schedule

The default interval for this script is 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Connection Failures	
Event Notification	
Raise event if the number of connection failures exceeds threshold?	Set to **Yes** to raise an event if the number of connection failures exceeds the threshold. The default is Yes.
Threshold - Maximum connection failures	Specify the maximum number of connections that can fail before an event is raised. The default is 15.
Event severity when the number of connection failures exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of connection failures exceeds the threshold. The default is 15.
Data Collection	
Collect data for the number of connection failures?	Set to **Yes** to collect data about the number of connection failures. The default is Yes.

HealthCheck

Use this Knowledge Script to monitor the active status of services on an OCS server. You can run this script on a Front-end server, a Mediation server, or an Edge server to monitor the services on that server.

Resource Object

OCS_ServicesObject

Default Schedule

The default interval for this script is one minute.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Services	
Start a service if it is stopped?	Set to **Yes** if you want to start a stopped service. The default is Yes.
Data Collection	
Collect data for service availability?	Set to **Yes** to collect data about service availability. The default is Yes.
Raise event if a service fails to start?	Set to **Yes** to raise an event if the service fails to start. The default is Yes.
Event severity when service fails to start	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the service fails to start. The default is 5.
Raise event if a stopped service has been started?	Set to **Yes** to raise an event if the service has been started. The default is Yes.
Event severity when a stopped service has been started	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when a stopped service has been started again. The default is 25.
Raise event if service is disabled?	Set to **Yes** to raise an event if the service is disabled. The default is No.
Event severity when service is disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the service is disabled. The default is 15.

MCUStatus

Use this Knowledge Script to monitor the health and draining state of a Multipoint Control Unit, or MCU. For example, IMMCU is an IM Conferencing server that runs as an IM service, and this script monitors the load for that server.

The different health states display the level of use as well as the number of users on the server.

Resource Object

OCS_MCUObject

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor MCU Health State	
Raise event if health state is Loaded?	Set to **Yes** to raise an event if the health state is considered to be *Loaded*. The default is unchecked.
Event severity when health state is Loaded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the health state is *Loaded*. The default is 20.
Raise event if health state is Full?	Set to **Yes** to raise an event if the health state is considered to be *Full*. The default is Yes.
Event severity when health state is Full	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the health state is *Full*. The default is 15.
Monitor MCU Draining State	
Raise event if health state is Requesting to Drain?	Set to **Yes** to raise an event if the health state is *Requesting to Drain*, or attempting to close MCU services to reduce the load. The default is Yes.
Event severity when health state is Requesting to Drain	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the draining state is *Requesting to Drain*. The default is 15.
Rase event if health state is Draining?	Set to **Yes** to raise an event if the health state is set to *Draining,* the process of closing MCU services to reduce the load. The default is Yes.
Event severity when health state is Draining	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the health state is set to *Draining*. The default is 10.

MediationServerCallActivity

Use this Knowledge Script to monitor inbound and outbound calls on a Mediation server. A Mediation server is an optional component that you will need if you connect OCS to a phone system, such as a PSTN, POTS, PBX, or some other legacy system.

Resource Object

OCS_MediationFolder

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Inbound Calls	
Event Notification	
Raise event if number of inbound calls exceeds threshold?	Set to **Yes** to raise an event if the number of inbound calls exceeds the threshold. The default is Yes.
Threshold - Maximum number of inbound calls	Specify the maximum number of inbound calls that can occur before an event is raised. The default is 15.
Event severity when the number of inbound calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of inbound calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for current inbound calls?	Set to **Yes** to collect data about the number of current inbound calls. The default is Yes.
Monitor Outbound Calls	
Event Notification	
Raise event if number of outbound calls exceeds threshold?	Set to **Yes** to raise an event if the number of outbound calls exceeds the threshold. The default is Yes.
Threshold - Maximum number of outbound calls	Specify the maximum number of outbound calls that can occur before an event is raised. The default is 15.
Event severity when the number of outbound calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of outbound calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for current outbound calls?	Set to **Yes** to collect data about the number of current outbound calls. The default is Yes.

Description	How to Set It
Monitor Rejected Inbound Calls	
Event Notification	
Raise event if number of rejected inbound calls exceeds threshold?	Set to **Yes** to raise an event if the number of rejected inbound calls exceeds the threshold. Calls can be rejected if the mediation server or the third-party gateway is over capacity. The default is Yes.
Threshold - Maximum number of rejected inbound calls	Specify the maximum number of rejected inbound calls that can occur before an event is raised. The default is 15.
Event severity when the number of rejected inbound calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of rejected inbound calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for rejected inbound calls?	Set to **Yes** to collect data about the number of rejected inbound calls. The default is Yes.
Monitor Rejected Outbound Calls	
Event Notification	
Raise event if number of rejected outbound calls exceeds threshold?	Set to **Yes** to raise an event if the number of rejected outbound calls exceeds the threshold. Calls can be rejected if the mediation server or the third-party gateway is over capacity. The default is Yes.
Threshold - Maximum number of rejected outbound calls	Specify the maximum number of rejected outbound calls that can occur before an event is raised. The default is 15.
Event severity when the number of rejected outbound calls exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of rejected outbound calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for rejected outbound calls?	Set to **Yes** to collect data about the number of current rejected outbound calls. The default is Yes.

MediationServerCallFailures

Use this Knowledge Script to monitor current call failure metrics for the Mediation server. A Mediation server is an optional component that you will need if you connect OCS to a phone system, such as a PSTN, POTS, PBX, or some other legacy system.

Resource Object

OCS_MediationObject

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Call Failures	
Event Notification	
Raise event if number of call failures exceeds threshold?	Set to **Yes** to raise an event if the number of call failures exceeds the threshold. The default is Yes.
Threshold - Maximum call failures	Specify the maximum number of calls that can fail before an event is raised. The default is 10 percent.
Event severity when number of call failures exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of call failures exceeds the threshold. The default is 10.
Data Collection	
Collect data for call failures?	Set to **Yes** to collect data about the number of call failures. The default is Yes.

MediationServerHealth

Use this Knowledge Script to track the global health of the Mediation server, an optional component that you will need if you connect OCS to a phone system, such as a PSTN, POTS, PBX, or some other legacy system. Health statuses include disabled, normal, light load, heavy load, and overload. The script also monitors total packet drops and TCP disconnects because the received packet is out of sync.

Resource Object

OCS_MediationFolder

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Health State	
Raise event if global health status is Heavy Load?	Set to **Yes** to raise an event if the global health status is heavy load. A health status of *Heavy Load* occurs when attempts to initiate new calls through the mediation server fail. The default is Yes.
Event severity when global health status is Heavy Load	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of conferences exceeds the threshold. The default is 15.
Raise event if global health status is Overloaded?	Set to **Yes** to raise an event if the global health status is *Overloaded*. The default is Yes.
Event severity when global health status is overloaded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of conferences exceeds the threshold. The default is 10.
Monitor Dropped RTP Packets	
Event Notification	
Raise event if number of dropped RTP packets exceeds threshold?	Set to **Yes** to raise an event if the number of dropped RTP packets exceeds the threshold. The default is Yes.
Threshold - Maximum dropped RTP packets	Specify the number of dropped RTP packets that can occur before an event is raised. The default is 5.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the threshold is exceeded. The default is 15.
Data Collection	
Collect data for dropped RTP packets per second?	Set to **Yes** to collect data about dropped RTP packets per second. The default is Yes.

Description	How to Set It
Monitor TCP Disconnects	
Event Notification	
Raise event if number of TCP disconnects exceeds threshold?	Set to **Yes** to raise an event if the number of TCP disconnects exceeds the threshold. The default is Yes.
Threshold - Maximum number of TCP disconnects	Specify the number of TCP disconnects that can occur before an event is raised. The default is 10.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the threshold is exceeded. The default is 10.
Data Collection	
Collect data for TCP disconnects?	Set to **Yes** to collect data about number of TCP disconnects. The default is Yes.

MediationServerUsage

Use this Knowledge Script to monitor the overall usage of the Mediation server, an optional component that you will need if you connect OCS to a phone system, such as a PSTN, POTS, PBX, or some other legacy system. Server usage data includes the number of overloaded conferences and the average time for processing audio packets.

Resource Object

OCS_MediationObject

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Overloaded Conferences	
Event Notification	
Raise event if the number of overloaded conferences exceeds threshold?	Set to **Yes** to raise an event if the number of overloaded conferences exceeds the threshold.The default is Yes.
Threshold - Maximum overloaded conferences	Specify the maximum number of overloaded conferences that can occur before an event is raised. The default is 50.
Event severity when overloaded conferences exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of overloaded conferences exceeds the threshold. The default is 15.
Data Collection	
Collect data for overloaded conferences?	Set to **Yes** to collect data about the number of overloaded conferences. The default is Yes.
Monitor Average Audio Packet Processing Time	
Event Notification	
Raise event if the average time exceeds threshold?	Set to **Yes** to raise an event if the average audio packet processing time exceeds the threshold. The default is Yes.
Threshold - Maximum average time	Specify the highest average processing time that can occur before an event is raised. The default is one second.
Event severity when average time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the average time exceeds the threshold. The default is 10.

Description	How to Set It
Data Collection	
Collect data for average time to process audio packets?	Set to **Yes** to collect data about the average processing time. The default is Yes.

SessionCallActivity

Use this Knowledge Script to monitor the session initiation rate for an OCS server. These sessions can include the following types: instant message (IM), file transfer, remote assistance, application sharing, audio, video, or telephony sessions.

This script gets session initiation data from the SessionDetails and Media Tables of the `LcsCDR` back-end database of the OCS Monitoring server. This script reports the number of sessions initiated per minute between two consecutive job iterations.

Note
In OCS, sessions have only two users, while conferences contain three or more users.

Resource Object

OCS_ArchivingAndCDRObject

OCS_CDRObject

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor IM Sessions	
Event Notification	
Raise event if number of IM sessions exceeds threshold?	Set to **Yes** to raise an event if the number of IM sessions exceeds the threshold. The default is Yes.
Threshold - Maximum IM sessions	Specify the maximum number of IM sessions that can occur before an event is raised. The default is 25.
Event severity when number of IM sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of IM sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for IM sessions?	Set to **Yes** to collect data about the number of IM sessions. The default is unchecked.
Monitor File Transfer Sessions	
Event Notification	

Description	How to Set It
Raise event if number of file transfer sessions exceeds threshold?	Set to **Yes** to raise an event if the number of file transfer sessions exceeds the threshold. The default is Yes.
Threshold - Maximum file transfer sessions	Specify the maximum number of file transfer sessions that can occur before an event is raised. The default is 25.
Event severity when number of file transfer sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of file transfer sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for file transfer sessions?	Set to **Yes** to collect data about the number of file transfer sessions. The default is unchecked.
Monitor Remote Assistance Sessions	
Event Notification	
Raise event if number of remote assistance sessions exceeds threshold?	Set to **Yes** to raise an event if the number of remote assistance sessions exceeds the threshold. The default is Yes.
Threshold - Maximum remote assistance sessions	Specify the maximum number of remote assistance sessions that can occur before an event is raised. The default is 25.
Event severity when number of remote assistance sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of remote assistance sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for remote assistance sessions?	Set to **Yes** to collect data about the number of remote assistance sessions. The default is unchecked.
Monitor Application Sharing Sessions	
Event Notification	
Raise event if number of application sharing sessions exceeds threshold?	Set to **Yes** to raise an event if the number of application sharing sessions exceeds the threshold. The default is Yes.
Threshold - Maximum application sharing sessions	Specify the maximum number of application sharing sessions that can occur before an event is raised. The default is 25.
Event severity when number of application sharing sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of application sharing sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for application sharing sessions?	Set to **Yes** to collect data about the number of application sharing sessions. The default is unchecked.
Monitor Audio Sessions	
Event Notification	
Raise event if number of audio sessions exceeds threshold?	Set to **Yes** to raise an event if the number of audio sessions exceeds the threshold. The default is Yes.
Threshold - Maximum audio sessions	Specify the maximum number of audio sessions that can occur before an event is raised. The default is 25.
Event severity when number of audio sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of audio sessions exceeds the threshold. The default is 15.

Description	How to Set It
Data Collection	
Collect data for audio sessions?	Set to **Yes** to collect data about the number of audio sessions. The default is unchecked.
Monitor Video Sessions	
Event Notification	
Raise event if number of video sessions exceeds threshold?	Set to **Yes** to raise an event if the number of video sessions exceeds the threshold. The default is Yes.
Threshold - Maximum video sessions	Specify the maximum number of video sessions that can occur before an event is raised. The default is 25.
Event severity when number of video sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of video sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for video sessions?	Set to **Yes** to collect data about the number of video sessions. The default is unchecked.
Monitor Telephony Sessions	
Event Notification	
Raise event if number of telephony sessions exceeds threshold?	Set to **Yes** to raise an event if the number of telephony sessions exceeds the threshold. The default is Yes.
Threshold - Maximum telephony sessions	Specify the maximum number of telephony sessions that can occur before an event is raised. The default is 25.
Event severity when number of telephony sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of telephony sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for telephony sessions?	Set to **Yes** to collect data about the number of telephony sessions. The default is unchecked.
Monitor Meeting Sessions	
Event Notification	
Raise event if number of meeting sessions exceeds threshold?	Set to **Yes** to raise an event if the number of meeting sessions exceeds the threshold. The default is Yes.
Threshold - Maximum meeting sessions	Specify the maximum number of meeting sessions that can occur before an event is raised. The default is 25.
Event severity when number of meeting sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of meeting sessions exceeds the threshold. The default is 15.
Data Collection	
Collect data for meeting sessions?	Set to **Yes** to collect data about the number of meeting sessions. The default is unchecked.

SessionCallFailures

Use this Knowledge Script to monitor session failure metrics for an OCS server. These sessions can include the following types: instant message (IM), file transfer, remote assistance, application sharing, audio, video, or telephony sessions.

Note
In OCS, sessions have only two users, while conferences contain three or more users.

This script calulates failed sessions from the SessionDetails and Media Tables of the `LcsCDR` back-end database of the OCS Monitoring server. This script reports the number of session failures per minute between two consecutive job iterations.

The SessionCallFailures script considers sessions with the following SIP Status codes as failed:

400, 401, 402, 403, 405, 406, 407, 408, 410, 413, 414, 415, 416, 420, 421, 423, 481, 482, 483, 485, 488, 493, 500, 501, 502, 503, 504, 505, 513, 600, 606

For mopre information about SIP status codes, see: www.rfc-ref.org/RFC-TEXTS/3261/chapter21.html.

Resource Object

OCS_ArchivingAndCDRObject

OCS_CDRObject

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Session Failures	
Event Notification	
Raise event if number of session failures exceeds threshold?	Set to **Yes** to raise an event if the number of session failures exceeds the threshold. The default is Yes.
Threshold - Maximum session failures	Specify the maximum number of session failures that can occur before an event is raised. The default is 5.
Event severity when number of session failures exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the number of session failures exceeds the threshold. The default is 15.

Description	How to Set It
Data Collection	
Collect data for session failures?	Set to **Yes** to collect data about the number of session failures. The default is No.

SystemUptime

Use this Knowledge Script to monitor how long a server remains up and running after a reboot.

Resource Object

OCS

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Raise event if system reboot detected?	Set to **Yes** to raise an event if the system has rebooted. The default is Yes.
Event severity when system reboot detected	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the system has rebooted. The default is 10.
Monitor System Uptime	
Data Collection	
Collect data for system uptime?	Set to **Yes** to collect data about system uptime, in hours. The default is Yes.

SystemUsage

Use this Knowledge Script to monitor the total CPU and memory usage on an OCS server and the contributions of each OCS service to this usage.

Resource Object

OCS_ServicesObject

OCS_ServicesFolder

Default Schedule

The default interval for this script is five minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the job fails. The default is 5.
Monitor Service CPU Usage	
Event Notification	
Raise event if service CPU usage exceeds threshold?	Set to **Yes** to raise an event if the percentage of total CPU usage for the service exceeds the threshold. The default is Yes.
Threshold - Maximum CPU usage	Specify the maximum percentage of the CPU that can be used by the service before an event is raised. The default is 65%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the maximum CPU usage for the service exceeds the threshold. The default is 15.
Data Collection	
Collect data for service CPU usage?	Set to **Yes** to collect data about CPU usage for the service. The default is Yes.
Monitor Total CPU Usage	
Event Notification	
Raise event if total CPU usage exceeds threshold?	Set to **Yes** to raise an event if the percentage of total CPU usage exceeds the threshold. The default is Yes.
Threshold - Maximum total CPU usage	Specify the maximum percentage of the total CPU that can be used before an event is raised. The default is 80%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the maximum CPU usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for total CPU usage?	Set to **Yes** to collect data about total CPU usage. The default is Yes.

Description	How to Set It
Monitor Service Memory Usage	
Event Notification	
Raise event if service memory usage exceeds threshold?	Set to **Yes** to raise an event if the percentage of total memory usage by the service exceeds the threshold. The default is Yes.
Threshold - Maximum service memory usage	Specify the maximum percentage of memory used by the service that can be used before an event is raised. The default is 65%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the maximum memory used by a the service exceeds the threshold. The default is 15.
Data Collection	
Collect data for service memory usage?	Set to **Yes** to collect data about total memory usage for the service. The default is Yes.
Monitor Total Memory Usage	
Event Notification	
Raise event if total memory usage exceeds threshold?	Set to **Yes** to raise an event if the percentage of total memory usage exceeds the threshold. The default is Yes.
Threshold - Maximum total memory usage	Specify the maximum percentage of the total memory that can be used before an event is raised. The default is 80%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event that is raised when the maximum total memory usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for total memory usage?	Set to **Yes** to collect data about total memory usage. The default is Yes.

Chapter 56
Oracle Knowledge Scripts

AppManager for Oracle Database on Windows provides the following Knowledge Scripts for monitoring Oracle Database resources. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AlertLog	Scans the Oracle Database Alert log for a search string that you specify.
BGProc	Monitors the total memory usage and the total number of physical read/write (I/O) operations per second for Oracle background processes.
Block	Monitors block-level database activity.
BlockingSessions	Monitors the number of user sessions that are blocking other processes from accessing the Oracle database.
Cache	Monitors the frequency with which requested data and resources are retrieved from the buffer cache, data dictionary, and library cache.
CallRate	Monitors the demand placed on a database instance from all sources.
CallsPerTransaction	Monitors the demand placed on a database instance by each transaction.
ConfigDB	Updates AppManager for Oracle Database with information about the Oracle databases you want to monitor.
ConsistentChangeRatio	Monitors the extent to which applications exercise the read consistency mechanism to ensure database consistency.
ContinuedRowRatio	Monitors rows that span more than one database block.
DatabaseDown	Monitors a database and its services to verify whether they are running.
DatafileSpace	Monitors the size of an Oracle datafile.
DiskSpaceAvail	Monitors the amount of disk space available for the archive log file, the background process log file, and user log files.
OpenCursors	Monitors the percentage of cursors opened per session, as well as the total number of cursors open in the system.
RecursiveToUserCallRatio	Monitors the ratio of recursive calls to overall database user calls.
RedoLogContention	Monitors the number of times that a process attempts to write an entry in the redo log buffer.
RedoLogSpaceWaitRatio	Monitors the redo log space wait ratio, which measures memory allocation.

Knowledge Script	What It Does
Report_BackgroundProcess	Generates a report about total memory use, and the total number of physical read/write operations per second for Oracle background processes.
Report_CacheHitRatio	Generates a report about buffer cache hit ratio, data dictionary hit ratio, and library cache hit ratio for Oracle servers.
Report_DatabaseAvailability	Generates a report about the up/down status of Oracle databases, and the OracleServer, OracleListener, and OracleStart services.
Report_DatafileSpace	Generates a report about the size (in MB) of Oracle Database data files.
Report_DiskSpaceAvailable	Generates a report about the amount of disk space (in MB) available for the archive, background process, and user log files.
Report_TablespaceAvailable	Generates a report about the free disk space available for tablespaces, disk space used by tables spaces, and the size of tablespaces.
Report_TransactionRate	Generates a report about the number of transactions per second for Oracle databases.
Report_UserLocks	Generates a report about the number of user-held locks on an Oracle database.
RollBackSegmentContention	Monitors the ratio of wait counts to total requests in the rollback segment.
RowSourceRatio	Monitors the row source ratio, which measures the percentage of rows that were retrieved using full table scans.
RunSql	Runs SQL statements.
SegmentExtentAvail	Monitors the percentage of extents (extensions of free space) available to each segment in a tablespace.
SortOverflowRatio	Monitors the sort overflow ratio, which measures the number of sorts that are using temporary segments.
SysStat	Retrieves statistics from the V$SYSSTAT table, which stores all the key statistics for a database instance.
TablespaceAvail	Monitors the percentage of disk space available to all the tablespaces in a database.
TopCpuUsers	Monitors the CPU time for current user sessions.
TopIOUsers	Monitors physical reads and writes (I/O) for current user sessions.
TopLockUsers	Monitors the current number of user-held locks on an Oracle database.
TopMemoryUsers	Monitors memory usage (User Global Area and PGA) for current user sessions.
TransactionRate	Monitors the transaction rate for an Oracle database.
UserCallsPerParse	Monitors the number of user calls per parse.
UserRollbackRatio	Monitors the user rollback ratio for an Oracle database, which indicates the percentage of attempted application transactions that fail.
UserSessions	Monitors the total number of user sessions accessing an Oracle database.

How Knowledge Scripts Access Oracle Databases

To gather the statistics and resource information needed to monitor an Oracle database, an Oracle Knowledge Script must log on to that database. The Oracle user account controls access to the Oracle Database. The Oracle user's Windows and SQL Server privileges have no effect on access to an Oracle database.

When you run a Knowledge Script on an Oracle database, you specify an Oracle user account that has been set up on that database for the *Username* parameter. The corresponding password is retrieved from the Oracle repository and sent, in encrypted format, to the AppManager agent on the Oracle Database server. The password is decrypted by the AppManager agent, which uses it to log on to the Oracle Database and run the Knowledge Script.

When you install the AppManager for Oracle Database module on an Oracle Database server, the setup program gathers a single Oracle Database user account name. In addition, it gathers the corresponding password for each database. The Oracle Database user account name must be the same on all databases, but each database can have a unique password associated with that user account.

Having a single Oracle user account is a requirement only to ensure that discovery succeeds. After discovery, you can use the Oracle user account gathered during installation to begin running Oracle Knowledge Scripts immediately, or you can use the AppManager Security Manager to store additional Oracle user account names and passwords in the AppManager repository.

Note
Oracle Knowledge Scripts provide one parameter for specifying an Oracle user account name to be used to log on to the databases you want to monitor. To run a single Knowledge Script job on multiple databases, each database must be configured with the same Oracle username.

AlertLog

Use this Knowledge Script to scan the Oracle Alert log for entries that match a search string that you specify. You can set a threshold for the maximum number of occurrences of the search string found during any single scan of the log file.

Each database maintains an Alert log file where it records database operations (such as creating or dropping a database) and error conditions (such as deadlocks). This Knowledge Script provides a general-purpose tool for scanning a database's alert log for specific entries.

When this Knowledge Script starts, it does not scan existing entries in the Alert log, and therefore it does not return any results or collect data on its first scan. As it continues to run at the intervals specified on the **Schedule** tab, this Knowledge Script scans the Alert log for any new entries created since the last scan. If, during any single scan, the number of matching entries exceeds the threshold you specify, the job raises an event. The detail message returns the number of occurrences of the search string found.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, this script returns the number of entries that matched the search string each time it scanned the Alert log. The default is n.
User name	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253

Description	How to Set It
Find (separate multiple strings with spaces)	Enter all or part of the string you want to search for. For this Knowledge Script, a “string” is any series of characters, not including spaces. You can specify multiple strings by separating each string with a space. For example, if you specify `ORA-600 ORA-1578`, the Knowledge Script searches for either of two “strings”: `ORA-600` or `ORA-1578`. The default values represent the most common Oracle error codes you might want to search for: • `ORA-600. Internal error`. • `ORA-1578. Block corruption`. • `ORA-60. Deadlock error`.
Case sensitive?	Enter **y** if you want the search to distinguish between uppercase and lowercase letters. When you enter y, the Knowledge Script finds only the occurrences whose capitalization matches the capitalization of the Find string. The default is n.
Exact match?	Enter **y** if you want the Knowledge Script to find only the entries that match the Find string exactly. For example, if you set this parameter to y and enter “`ORA-60`” as the Find string, only “`ORA-60`” is considered a match. If you set this parameter to n and search for “`ORA-60`”, entries that contain “`ORA-60`”, such as “`ORA-600`”, are considered a match. The default is n.
Maximum threshold for occurrences found	Specify the maximum number of occurrences allowed during any single scan of the Alert log. If the number of occurrences of the Find string exceeds this threshold, an event is raised. The default is 1.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

BGProc

Use this Knowledge Script to monitor the total memory usage and the total number of physical read/write (I/O) operations per second for Oracle background processes. You can configure this Knowledge Script to monitor memory usage, read/write operations, or both. If the background processes being monitored exceed the threshold you set for total memory usage or the total number of read/write operations per second, this Knowledge Script raises an event.

Oracle background processes include `CKPT`, `DBW0`, `LGWR`, `PMON`, `RECO`, `SMON`, `SNP0`, and others. You can monitor all background processes or selected background processes.

Resource Objects

Oracle Server folder, Oracle Database icon.

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script collects the statistics you are monitoring: the total number of read/write operations per second, the total memory usage, or both, for all monitored background processes. The default is n.
User name	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Monitor read/write operations?	Set to **y** to monitor the number of physical read/write operations per second by background processes. When set to n, the Knowledge Script does not monitor this statistic (regardless of whether a threshold is specified) and does not collect data. The default is y.
Maximum threshold for read/write operations	Enter a threshold for the maximum number of physical read/write operations per second. The default is 50 read/write operations.
Monitor memory usage?	Set to **y** to monitor the memory usage by background processes. When set to n, the Knowledge Script does not monitor this statistic (regardless of whether a threshold is specified) and does not collect data. The default is y.
Maximum threshold for memory usage	Enter a threshold, in megabytes, for the maximum amount of memory used by all background processes you are monitoring. The default is 50 MB.

Description	How to Set It
Oracle background processes to monitor	Specify the names of the background processes you want to monitor. Separate the names with commas; do not use spaces. To monitor all Oracle background processes, enter an asterisk (*). Possible valid background process names include: • CKPT • DBW0 • LGWR • PMON • RECO • SMON • SNP0 • SNP1 The default is all (*) background processes.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Block

Use this Knowledge Script to monitor block-level database activity. Oracle data blocks are the smallest unit of storage for a database; monitoring I/O activity at the block level can be a key performance indicator.

Use this Knowledge Script to monitor any combination of these statistics:

- **The number of block changes per transaction.** This block change rate measures the number of SQL Data Manipulation Language (DML) commands that each transaction performs (for example, to create and drop indexes). As the number of block changes increases, the efficiency of the database transaction and database performance decreases.
- **The number of times the Oracle Buffer Manager locates a database block per second.** This *block get* rate indicates the rate at which an application references the database. An increase in the block get rate suggests an increase in overall server load. A decrease in the block get rate without a decrease in load may indicate that you need to do some database tuning because there has been a slowdown in the number of database blocks requested and located per second.
- **The number of times database blocks are requested per committed transaction.** This *block visit* rate measures the database work load per completed transaction (including both successful and aborted database transactions).

You can set a threshold for each statistic you choose to monitor. If any threshold is exceeded, the Knowledge Script raises an event.

Resource Objects

Oracle Server folder, Oracle Database icon.

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script collects the statistics you choose to monitor: the number of block changes per transaction, the number of block get operations per second, and/or the number of block visits per transaction. The default is n.

Description	How to Set It
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Monitor block change rate?	Set to **y** to monitor the number of block changes per transaction. When set to n, the Knowledge Script does not monitor this statistic (regardless of whether a threshold is specified) and does not collect data. The default is y.
Maximum threshold for block changes	Enter a threshold for the maximum number of block changes per transaction. The default is 100 changes per transaction.
Monitor block get rate?	Set to **y** to monitor the number of times the Oracle Buffer Manager locates a database block per second. When set to n, the Knowledge Script does not monitor this statistic (regardless of whether a threshold is specified) and does not collect data. The default is y.
Maximum threshold for block gets	Enter a threshold for the maximum number of block get operations per second. The default is 100 `get` operations per second.
Monitor block visit rate?	Set to **y** to monitor the number of times database blocks are requested per committed transaction. When set to n, the Knowledge Script does not monitor this statistic (regardless of whether a threshold is specified) and does not collect data. The default is y.
Maximum threshold for block visits	Enter a threshold for the maximum number of block get operations per committed transaction. The default is 100 operations per committed transaction.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

BlockingSessions

Use this Knowledge Script to monitor the user sessions that are blocking other sessions and processes from accessing the Oracle Database. You can set a threshold for the number of sessions that are allowed to block other sessions and processes. If the number of blocking sessions exceeds this threshold, an event is raised.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script collects the number of blocking sessions found. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for number of blocking sessions	Enter a threshold for the maximum number of user sessions allowed to block other processes. The default is 10 sessions.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Cache

Use this Knowledge Script to monitor the frequency with which requested data and resources are retrieved from the cache. As this *hit ratio* (that is, the percentage of time that data or resources are retrieved from the cache) decreases, performance also decreases because Oracle must retrieve data from disk or reinitialize library objects in order to service the requests.

Use this Knowledge Script to monitor any combination of these statistics:

- The buffer cache hit ratio indicates the percentage of time that requested data is found in the Oracle buffer cache. This statistic reflects the effectiveness of the buffer cache and database performance.
- The data dictionary hit ratio indicates the percentage of time that requested data is found in the data dictionary. This statistic reflects the effectiveness of the data dictionary and database performance.
- The library cache hit ratio reflects the percentage of time that system pin requests to access objects in the library cache can be serviced without reinitializing or reloading library objects. Changes to the library cache hit ratio may occur when an application comes active, causing more SQL statements and stored procedures to be used.

You can set a threshold for each cache hit ratio you choose to monitor. If a cache hit ratio is less than any threshold you set, this Knowledge Script raises an error.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script collects the statistics you choose to monitor: the buffer cache hit ratio, the data dictionary hit ratio, and/or the library cache hit ratio. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.

Description	How to Set It
Monitor buffer cache hit ratio?	Set to **y** to monitor the percentage of time that requested data is found in the Oracle buffer cache. When set to n, the Knowledge Script does not monitor this statistic (regardless of whether a threshold is specified) and does not collect data. The default is y.
Minimum threshold for buffer cache hit ratio	Enter a minimum percentage for the buffer cache hit ratio. If the actual hit ratio is lower than this threshold, an event is raised. Ideally, this percentage should be set relatively high, because the more frequently Oracle uses the buffer, the better your database performance. When the actual hit ratio falls below the threshold you set, the event alerts you that database performance has degraded. The default is 70%.
Monitor data dictionary hit ratio?	Set to **y** to monitor the percentage of time that requested data is found in the data dictionary. When set to n, the Knowledge Script does not monitor this statistic (regardless of whether a threshold is specified) and does not collect data. The default is y.
Minimum threshold for data dictionary hit ratio	Enter a minimum percentage for the data dictionary hit ratio. If the actual hit ratio is lower than this threshold, an event is raised. Ideally this percentage should be set high, because the more frequently Oracle uses the data dictionary to service requests, the better your database performance. When the actual hit ratio falls below the threshold you set, the event alerts you that database performance has degraded. The default is 90%.
Monitor library cache hit ratio?	Set to **y** to monitor the percentage of time that system pin requests to access objects in the library cache can be serviced without reinitializing or reloading library objects. When set to n, the Knowledge Script does not monitor this statistic (regardless of whether a threshold is specified) and does not collect data. The default is y.
Minimum threshold for library cache hit ratio	Enter a minimum percentage for the library cache hit ratio. If the actual hit ratio is lower than this threshold, an event is raised. Ideally, this percentage should be set extremely high because reinitializing or reloading library objects imposes a large performance hit. When the actual hit ratio falls below the threshold you set, the event alerts you that database performance has degraded. The default is 99%
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

CallRate

Use this Knowledge Script to monitor the demand placed on a database instance from all sources. This demand is determined by tracking the number of database calls per second from all applications and processes accessing the database instance. The database calls tracked include Parse, Execute, and Fetch statements. These calls are sometimes described as **user calls**. When the call rate (and thus the workload demand on the server) exceeds the threshold you set, an event is raised.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the total user calls per second for all work sources. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for call rate	Enter a threshold for the maximum number of calls per second. The default is 100 calls per second.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

CallsPerTransaction

Use this Knowledge Script to monitor the demand placed on a database instance by each transaction. This demand is determined by tracking the number of database calls (for example, to parse, execute, and fetch data) per committed transaction. When the number of database requests per transaction exceeds the threshold you set, an event is raised.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the number of database calls per transaction. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for calls per transaction	Enter a threshold for the maximum number of calls per transaction. The default is 100 calls per transaction.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

ConfigDB

Use this Knowledge Script to update AppManager for Oracle Database with the username, password, and additional system settings for the database that you want to monitor. If there is an error updating the AppManager for Oracle Database repository, an event is raised.

Note that when you install AppManager for Oracle Database, this information is automatically gathered for all existing Oracle databases. You only need to run this Knowledge Script on any Oracle databases that you add after installing AppManager for Oracle Database.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is n.
Management server computer name	Specify the name of the computer on which the AppManager for Oracle Database management server is installed.
Database names	Specify the name of the Oracle database that you want to be managed by AppManager for Oracle Database. You can specify a single database name, or specify multiple database names separated by commas. You can also enter an asterisk (*) to represent all Oracle databases. The default database name is `*`.
Oracle Username	Specify the Oracle Username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Password for Oracle Username	Specify the Oracle password for the user specified in the Oracle Username parameter.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

ConsistentChangeRatio

Use this Knowledge Script to monitor the extent to which applications exercise the read consistency mechanism to ensure database consistency.

The consistent change ratio is based on the number of requested database blocks that have changed since a read consistency point was taken as part of a query. When the ratio of changed database blocks to all requested database blocks exceeds the threshold you set, an event is raised.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the percentage of requested database blocks that changed since the read operation. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for consistent change ratio	Enter a threshold for the maximum number of consistent read changes that should be allowed before generating an event. The default is 100.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

ContinuedRowRatio

Use this Knowledge Script to monitor rows that span more than one database block. This Knowledge Script monitors the ratio of **continued rows** that span more than one database block to all rows fetched. In most cases, this ratio should be close to zero. If the continued row ratio increases over time (indicating that more and more rows span multiple database blocks), it may mean that the `PCTFREE` storage parameter is set too low for one or more tables.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the continued row ratio. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for continued row ratio	Enter a threshold for the ratio of continued rows to all rows fetched. The default ratio is 01.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

DatabaseDown

Use this Knowledge Script to monitor the status of a database and its associated OracleServer service.

It is possible for the OracleServer service to be running while its associated database is down. This Knowledge Script monitors the database and its OracleServer service at the same time and raises an event if it discovers that either one is not running.

In addition, you have the option of monitoring the Oracle Listener service (there is a single instance of this service per Oracle Server) and the OracleStart service associated with the database and raising an event if either one is down.

Note
Not all versions of Oracle include the OracleStart service. If you are using a version of Oracle that does not include the OracleStart service, the Oracle managed object automatically ignores any requests from the Knowledge Script to monitor this service. If the *Monitor the OracleStart service?* parameter is set to y, but the OracleStart service does not exist in the version of Oracle you are using, the Knowledge Script does not raise an event.

The detail message indicates which the database or associated services are down.

Resource Objects

Oracle Server icon, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the value 100 every time it finds a resource is up and the value 0 every time it finds a resource is down. This provides a way to report on the percentage of system up time in any given period. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default user name is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.

Description	How to Set It
Monitor the OracleStart service?	Enter **y** to monitor the status of the `OracleStart` service associated with the database. If the service exists in your version of Oracle but is not running, an event is raised. Note that if you are using a version of Oracle that does not include the `OracleStart` service, the Oracle managed object automatically ignores any requests from the Knowledge Script to monitor this service, and no event is raised. The default is n.
Monitor the Oracle Listener service?	Check **Yes** to monitor the status of the Oracle Listener service. If the service is not running, an event is raised. The default is no.
Name of Listener Service	Specify the name of an Oracle listener service when there is only one such listener used among multiple databases. This listener service's status is checked for each of the databases upon which the job is run.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

DatafileSpace

Use this Knowledge Script to monitor the size of an Oracle database's datafile. When the size of the datafile (in megabytes) exceeds the threshold you set, an event is raised.

Resource Objects

Oracle Database icon, datafile icon.

Note
When run on an Oracle Database icon, a single Knowledge Script job monitors every datafile for that database. When run on a single datafile icon, a single Knowledge Script monitors just that datafile.

Default Schedule

The default interval for this script is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the current size of the datafile (in MB). The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for a datafile	Enter a threshold, in megabytes, for the maximum size of a datafile. The default is 20 MB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

DiskSpaceAvail

Use this Knowledge Script to monitor the amount of disk space available for the archive log file, the background process log file, and user log files of a database. You can monitor the space available for all three or any combination. For example, you could turn off monitoring for the archive log and background process log files and monitor just the disk space available for the user logs.

For each type of log file, you can set a minimum threshold. If the amount of available disk space is less than any of the thresholds you set for a specific type of log file, the Knowledge Script raises an event.

Resource Objects

Oracle Server icon, Oracle Database icon.

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 1 hour.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, this script returns the amount of free disk space for each type of log file that you are monitoring. The script returns only the data being monitored. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Monitor space available for the archive log?	Enter **y** to monitor the amount of disk space available for the database's archive log file. When set to n, the Knowledge Script does not monitor this statistic (regardless of whether a threshold is specified) and does not collect data. The default is y.
Minimum threshold for archive log space	Specify the minimum amount of available disk space for the archive log file. If the amount of available space is less than this number, an event is raised. The default is 100.

Description	How to Set It
Monitor space available for background process log?	Enter **y** to monitor the amount of space available for the database's background process log file. When set to n, the Knowledge Script does not monitor this statistic (regardless of whether a threshold is specified) and does not collect data. The default is y.
Minimum threshold for background process log space	Specify the minimum amount of available disk space for the background process log file. If the amount of available space is less than this number, an event is raised. The default is 100.
Monitor space available for user logs?	Enter **y** to monitor the amount of space available for the database's user log files. When set to n, the Knowledge Script does not monitor this statistic (regardless of whether a threshold is specified) and does not collect data. The default is y.
Minimum threshold for user log space	Specify the minimum amount of available disk space for user log files. If the amount of available space is less than this number, an event is raised. The default is 100.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

OpenCursors

Use this Knowledge Script to monitor the percentage of cursors opened per session, as well as the total number of cursors open in the system. In the Oracle environment, a **cursor** is a type of handle, or pointer, used to identify a query in the system. Cursors can be opened by users or by the system itself. A high number of open cursors can be caused by a programming error, and may result in performance problems. In the `init.ora` file, you can specify the maximum number of cursors that may be opened by a session.

In this Knowledge Script, you can specify a threshold for the maximum percentage of open cursors allowed per session. Note that this is a percentage of the number specified in the `open_cursor` parameter in the `init.ora` file. For example, the `init.ora` file specifies that 60 cursors may be open in a session. In the Knowledge Script, you specify a threshold percentage of 75%. In this case, the Knowledge Script raises an event when 75% of the 60 allowed cursors (or 45 cursors) are open in any session. You can also specify a threshold for the total number of open cursors allowed in the system. An event is raised if either threshold is exceeded.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script collects the statistics you choose to monitor: the percentage of open cursors per session, and the total number of open cursors in the system. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Number of open cursors in the system	Specify the total number of cursors that may be open in the system. The default is 1000.

Description	How to Set It
Percentage of cursors opened per session	Specify the percentage of open cursors allowed per session. Note that this percentage is based on the number of open cursors allowed per session specified in the `init.ora` file. The default is 80%.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

RecursiveToUserCallRatio

Use this Knowledge Script to monitor the ratio of recursive calls to overall database user calls. A change in this ratio can reflect an application change or indicate a need to adjust the size of the shared pool. You can specify a ratio threshold. If the recursive-to-user call ratio exceeds the threshold you set, an event is raised.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the recursive-to-user call ratio. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for recursive-to-user-call ratio	Enter a threshold for the maximum change in the recursive-to-user call ratio. The previous ratio is compared with the current ratio, and the difference is compared to the threshold. The default ratio is 10.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

RedoLogContention

Use this Knowledge Script to monitor the number of times that a process tries to write an entry in the redo log buffer. The number of retries should be low. A high number of retries can adversely affect system performance, as processes must wait for buffers. If a process has to make numerous attempts to write an entry in the redo log buffer, you may need to allocate more space to the redo log buffer.

You can set a threshold value for the maximum number of times a process can try to write an entry in the redo log buffer. If the number of retries exceeds the threshold you set, an event is raised.

Resource Objects

Oracle Server folder, Oracle Database icon.

Note
When run on the Oracle Server folder, a single Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a single Knowledge Script monitors just that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script collects the number of times that processes attempted to write entries to the redo log buffer. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for redo log buffer allocation retries	Enter a threshold for the maximum number of times that a process tries to write an entry to the redo log buffer. The default is 50.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

RedoLogSpaceWaitRatio

Use this Knowledge Script to monitor the redo log space wait ratio. The redo log space wait ratio measures memory allocation. The ratio reflects how often a server process had to wait before writing an entry in the redo log buffer. If this ratio increases, you may want to increase the size of the redo log buffer. When the redo log space wait ratio exceeds the threshold you set, an event is raised.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the redo log space wait ratio. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for redo log space wait ratio	Enter a threshold for the redo log wait ratio. The default ratio is 0.0002.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_BackgroundProcess

Use this Report script to generate a report about total memory use, and the total number of physical read/write operations per second for Oracle background processes. This report allows you to make a statistical analysis of the data point values (for example, the average or maximum value over a time period).

This report uses data collected by the BGProc Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time period covered by the report • **Minimum**: The minimum value of data points for the time period covered by the report • **Maximum**: The maximum value of data points for the time period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time period covered by the report • **Close**: The last value for the time period covered by the report • **Change**: The difference between the first and last values for the time period covered by the report (close - open = change) • **Count**: The number of data points for the time period covered by the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.

Description	How to Set It
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_CacheHitRatio

Use this Oracle_Report script to generate a report about buffer cache hit ratio, data dictionary hit ratio, and library cache hit ratio for Oracle servers. This report allows you to make a statistical analysis of the data point values (for example, the average or maximum value over a time period).

This report uses data collected by the Cache Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time period covered by the report • **Minimum**: The minimum value of data points for the time period covered by the report • **Maximum**: The maximum value of data points for the time period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time period covered by the report • **Close**: The last value for the time period covered by the report • **Change**: The difference between the first and last values for the time period covered by the report (close - open = change) • **Count**: The number of data points for the time period covered by the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.

Description	How to Set It
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_DatabaseAvailability

Use this Oracle_Report script to generate a report about the up/down status of Oracle databases, and the `OracleServer`, `OracleListener`, and `OracleStart` services.

This report uses data collected by the DatabaseDown Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Data settings	
Hours or percentage on chart	Select whether to illustrate availability by hours or by percentage.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.

Description	How to Set It
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_DatafileSpace

Use this Oracle_Report script to generate a report about the size (in MB) of Oracle Database data files. This report allows you to make a statistical analysis of the data point values (for example, the average or maximum value over a time period).

This report uses data collected by the DatafileSpace Knowledge Script.

Resource Objects

Report Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time period covered by the report • **Minimum**: The minimum value of data points for the time period covered by the report • **Maximum**: The maximum value of data points for the time period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time period covered by the report • **Close**: The last value for the time period covered by the report • **Change**: The difference between the first and last values for the time period covered by the report (close - open = change) • **Count**: The number of data points for the time period covered by the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.

Description	How to Set It
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_DiskSpaceAvailable

Use this Oracle_Report script to generate a report about the amount of disk space (in MB) available for the archive, background process, and user log files. This report allows you to make a statistical analysis of the data point values (for example, the average or maximum value over a time period).

This report uses data collected by the DiskSpaceAvail Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time period covered by the report • **Minimum**: The minimum value of data points for the time period covered by the report • **Maximum**: The maximum value of data points for the time period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time period covered by the report • **Close**: The last value for the time period covered by the report • **Change**: The difference between the first and last values for the time period covered by the report (close - open = change) • **Count**: The number of data points for the time period covered by the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.

Description	How to Set It
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. A timestamp lets y ou run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_TablespaceAvailable

Use this Oracle_Report script to generate a report about the free disk space available for tablespaces, disk space used by tables spaces, and the size of tablespaces. This report allows you to make a statistical analysis of the data point values (for example, the average or maximum value over a time period).

This report uses data collected by the TablespaceAvail Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time period covered by the report • **Minimum**: The minimum value of data points for the time period covered by the report • **Maximum**: The maximum value of data points for the time period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time period covered by the report • **Close**: The last value for the time period covered by the report • **Change**: The difference between the first and last values for the time period covered by the report (close - open = change) • **Count**: The number of data points for the time period covered by the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.

Description	How to Set It
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_TransactionRate

Use this Oracle_Report script to generate a report about the number of transactions per second for Oracle databases. This report allows you to make a statistical analysis of the data point values (for example, the average or maximum value over a time period).

This report uses data collected by the TransactionRate Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time period covered by the report • **Minimum**: The minimum value of data points for the time period covered by the report • **Maximum**: The maximum value of data points for the time period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time period covered by the report • **Close**: The last value for the time period covered by the report • **Change**: The difference between the first and last values for the time period covered by the report (close - open = change) • **Count**: The number of data points for the time period covered by the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.

Description	How to Set It
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Click in the Value column, and click the **Browse [...]** button to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_UserLocks

Use this Oracle_Report script to generate a report about the number of user-held locks on an Oracle database. This report allows you to make a statistical analysis of the data point values (for example, the average or maximum value over a time period).

This report uses data collected by the TopLockUsers Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time period covered by the report • **Minimum**: The minimum value of data points for the time period covered by the report • **Maximum**: The maximum value of data points for the time period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time period covered by the report • **Close**: The last value for the time period covered by the report • **Change**: The difference between the first and last values for the time period covered by the report (close - open = change) • **Count**: The number of data points for the time period covered by the report
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Enter a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.

Description	How to Set It
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **yes** to append a timestamp to the title of the report, making each title unique. The timestamp is made up of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

RollBackSegmentContention

Use this Knowledge Script to monitor rollback segment contention for a database. In the Oracle environment, the **rollback segment** is a temporary location where changes are stored until the user makes the changes permanent. This Knowledge Script compares the number of requests waiting to access data from the rollback segment to the total number of requests for data during the monitoring interval. In the Knowledge Script, you can specify the maximum percentage of requests allowed to wait for data from the rollback segment. If the percentage of waiting requests exceeds the threshold you specify, an event is raised. If you find that too many processes are waiting to access the rollback segment, you may need to create additional rollback segment.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. The data is stored in the AppManager for Oracle Database repository. When set to y, the script collects the number of requests waiting to access the rollback segment. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Percentage of unsuccessful requests	Specify the percentage of total requests that may be waiting to access data from the rollback segment. The default is 1%.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5.

RowSourceRatio

Use this Knowledge Script to monitor the row source ratio. This ratio measures the percentage of rows that were retrieved using full table scans. Because a full table scan is less efficient than retrieving rows by row ID, this ratio gives you an indication of potential performance problems. If you observe an increase in this ratio, you may want to review other statistics to find the source of the problem. When this ratio exceeds the threshold you set, an event is raised.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the ratio of rows retrieved using a full table scan. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for row source ratio	Enter a threshold for the row source ratio. The default ratio is .25.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

RunSql

Use this Knowledge Script to run a SQL statement. You can enter the SQL statement to be executed when you run this Knowledge Script, or you can load the statement from a script file. You specify the column to monitor and whether to monitor the value found in the column or the value's rate of change (changes per second).

Note
There is no syntax-checking mechanism from the Operator Console. Syntax checking is done by the Oracle server on the managed client when the job runs. If an error is detected, the Oracle server returns the error result to the Knowledge Script, and the job stops.

Resource Objects

Oracle Server folder, Oracle Database icon.

Note
When run on the Oracle Server folder, a single Knowledge Script job runs the SQL statements on every database on that server. When run on a single Oracle Database icon, a single Knowledge Script runs the SQL statements just on that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is n.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, this script returns the number of rows returned from the SQL statement. If you choose to monitor the column's rate of change and set this parameter to y, the script returns the change in the number of rows since the last time the SQL statement was run. The default is y.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253. **Note** In general, permission to run specific SQL commands and statements is derived from the permissions granted to the user account name you are using to run this Knowledge Script.
Load SQL script from file?	Set to **y** to load the SQL statement from a file. Set to n to enter the SQL statement in the **SQL statement** field. The default is n.

Description	How to Set It
SQL script file (full path)	If you set the **Load SQL script** parameter to **y**, enter the complete path to the file that contains the SQL statement. For example: `F:\netiq\Sample.sql` **Note** If the AppManager for Oracle Database agent service (`NetIQmc`) is running as a system account, you cannot enter a path in UNC format (such as *machine**dir**Sample.sql*).
SQL statement	If you set the **Load SQL script** parameter to n, enter the SQL statement to be executed. The default statement selects all processes from the `V$PROCESS` table. **Tip:** Unless you are entering very simple queries, you may find typing a SQL statement into this field is error-prone. To avoid this, use the **SQL script file** parameter. Alternatively, if you have an AppManager for Oracle Database Developer's license, you can check this Knowledge Script out of the repository, use the Knowledge Script Editor to paste the desired SQL statement into the **SQL statements** field, and then check the modified Knowledge Script back in.
Select column by column number?	Set to **y** to select a column by column number. Set to n to select a column by column name. The default is y (column number).
Column number	If you set the **Select column by column number?** parameter to **y**, enter the column number to use as the primary output value (the column you specify must contain numeric data). Entering 0 returns the number of rows returned from the SQL statement. Any other positive value returns the value for the specified column's first row of data. If the specified column is not a numeric field, an error is raised and the Knowledge Script returns an error.
Column name	If you set the **Select column by column number?** parameter to n, enter the column name to use as the primary output value (the column you specify must contain numeric data). The value for the specified column's first row of data is returned. If the specified column is not a numeric field, an error is raised and the Knowledge Script returns an error.
Legend	Enter a legend for the output of your SQL statement. The default is blank. If you leave this parameter blank, AppManager for Oracle Database constructs a legend based on the column number. For example, if the column number is 0, the constructed legend is "`# Result Rows`". If the column number is greater than 0, the constructed legend is the specified column heading. If no heading exists, the constructed legend is: "`Column <num> Value`"
Monitor the column's rate of change?	Set to **y** to monitor the number of times the column's value changes per second. Set to n to monitor the actual value found in the column. The default is n.
Condition: <, =, or >	Indicate the condition (less than, equal to, or greater than) you want to check for. This parameter is used in conjunction with the threshold parameter to control when events are raised. The default is greater than (>).

Description	How to Set It
Value or rate threshold	Enter a threshold for the value you are monitoring. Depending on how you set the **Calculate column change rate?** parameter, this may indicate a threshold for the statistic's value or for the number of times the value changes per second. The value you set here is used in conjunction with the **Condition: <, =, or >** parameter to control when events are raised. The default is 1000.
Number of rows to be displayed	Specify the number of rows you want displayed in the detail message (event or data). The default is 5 rows. **Note** You can enter 0 to indicate no limit (keep all output rows). However, currently the detail message is limited to 32K characters.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Loading a SQL statement from a Script File

In many cases, you may find it useful to run a complex SQL statement using a SQL script file rather than entering the statement directly in the **SQL statement** parameter.

The example below illustrates how to use a SQL script loaded from a file to perform a custom monitoring task. This example monitors tablespaces, and collects the following information:

- Largest free extent in the tablespace.
- Number of free extents in the tablespace.
- Total free space in the tablespace.
- Percentage of the tablespace's available space that is free.

If the percentage of available tablespace is less than 5%, an event is raised. Here's how the key Knowledge Script parameters are set:

This Parameter:	Is Set to:
Event?	y
Collect data?	y
Load SQL script from file?	y
SQL script file (full path)	`D:\netiq\tblspace.sql`
Select column by column number?	y
Column number	5
Column name	pct_free
Legend	Percentage Free
Calculate column change rate?	n
Condition: <, =, or >	<
Value or rate threshold	5

The `tblspace.sql` script file contains the following SQL statement:

```
SELECT Tablespace_Name, Max_Blocks, Count_Blocks,
       Sum_Free_Blocks,
```

```
       100*Sum_Free_Blocks/Sum_Alloc_Blocks AS pct_free
FROM
       (SELECT Tablespace_Name, SUM(Blocks) Sum_Alloc_Blocks
       FROM dba_data_files GROUP BY Tablespace_Name),
       (SELECT Tablespace_Name FS_TS_NAME, MAX(Blocks)
       AS Max_Blocks, COUNT(Blocks) AS Count_Blocks,
       SUM(Blocks) AS Sum_Free_Blocks
       FROM dba_free_space GROUP BY Tablespace_Name)
WHERE Tablespace_Name = FS_TS_NAME
ORDER BY pct_free
```

SegmentExtentAvail

Use this Knowledge Script to monitor the percentage of extents (extensions of free space) available to each segment in a tablespace. You can set a threshold value for the minimum percentage of extents that should be available for each segment. For example, you may want each segment to have at least 70% of extents available. In addition, you can set a threshold for the maximum number of segments allowed to fall below this percentage before an event is raised. For example, you specify that 70% of extents should be available for each segment, and that 4 segments should be the maximum number of segments allowed to have less than 70% of their extents available. If 4 segments are found to have less than 70% of their extents available, an event is raised.

It is important to note that an event is raised only when *both* conditions are met. In the example described above, AppManager for Oracle Database would not raise an event until 4 segments were found that had less than 70% of their extents available.

Resource Objects

Oracle Server folder, Oracle Database icon.

Note
When run on the Oracle Server folder, a single Knowledge Script job runs the SQL statements on every database on that server. When run on a single Oracle Database icon, a single Knowledge Script runs the SQL statements just on that database.

Default Schedule

The default interval for this script is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, this script returns the number of segments that have less than the specified percentage of extents available. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253. **Note** In general, permission to run specific SQL commands and statements is derived from the permissions granted to the user account name you are using to run this Knowledge Script.
Min. % of available extents for each segment	Specify the minimum percentage of extents available for each segment in a tablespace. The default is 80%.

Description	How to Set It
Max. segments with more than above % of extents allocated	Specify the maximum number of segments allowed to have less than the specified percentage of extents available. The default is 5 segments.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

SortOverflowRatio

Use this Knowledge Script to monitor the sort overflow ratio. This ratio measures the number of sorts that are using temporary segments. An increase in this ratio indicates that more sort operations need to allocate work space on disk. If most sorts are of a moderate size, you may want to increase the sort area size to accommodate them. If the ratio exceeds the threshold you set, an event is raised.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. When set to y, the script returns the ratio of the number of sorts using temporary segments versus the number that do not. For example, a ratio of .75 indicates that 3 out of 4 sorts are using temporary segments. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for sort overflow ratio	Enter a threshold for the sort overflow ratio The default ratio is 0.75.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

SysStat

Use this Knowledge Script to retrieve statistics from a database's V$SYSSTAT table. This table stores all the key statistics for a database. You specify the statistic to monitor and the value and condition to check for. You can monitor either the statistic's **value** or **change rate** (changes per second) to raise an event.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the current value of each specified statistic at each interval. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
V$SYSSTAT name	Specify the name of the statistic you want to monitor. For example, `USER CALLS`. For information about the fields in the V$SYSSTAT table, see your Oracle documentation (for example, Oracle8 Reference, Appendix C Statistics Descriptions). The default statistic is `EXECUTE COUNT`.
Monitor statistic's change rate?	When this parameter is set to **y**, the Knowledge Script monitors the number of times the statistic's value changes per second. When this parameter is set to n, the Knowledge Script monitors the value of the statistic. The default is y.
Condition: <, =, or >	Indicate the condition (less than, equal to, or greater than) you want to check for. This parameter is used in conjunction with the **Value or rate threshold** parameter to control what raises an event. The default is greater than (>).

Description	How to Set It
Value or rate threshold	Enter a threshold value for the specified statistic. Depending how you set the **Monitor statistic's change rate?** parameter, this may indicate a threshold for the statistic's value or for the number of changes per second. The value you set here is used in conjunction with the **Condition (<, =, or >)** parameter to control what raises an event. The default is 100.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Example of How This Script is Used

You can use this Knowledge Script to monitor either a statistic's **value** or its **change rate** (changes per second). To do this, you need to specify:

- The statistic to monitor
- Whether you want to monitor a value or a change rate
- The type of threshold condition for which you are monitoring (less than, greater than, or equal to)
- The value or change rate threshold

For example, to generate an event when there are more than 100 `Execute` calls in a monitoring interval:

This Parameter	Is Set to
Event?	y
V$SYSSTAT name	execute count
Monitor statistic's change rate?	n
Condition (<, =, or >)	>
Value or rate threshold	100

In some cases, monitoring a statistic's change rate is even more useful in measuring database performance and application efficiency than monitoring for a current value. For example, if the change rate for a statistic such as **execute count** begins to drop (with fewer execute statements processed per second), it suggests a performance bottleneck.

Consult your Oracle documentation for recommendations on setting thresholds for specific statistics.

TablespaceAvail

Use this Knowledge Script to monitor the disk space used by tablespaces.

This Knowledge Script can monitor:

- The amount of free disk space available for a tablespace as a percentage, as an absolute amount, or both.
- The amount of disk space used by a tablespace as a percentage, as an absolute amount, or both.
- The size of a tablespace.

This Knowledge Script monitors the disk space allocated to Oracle, not the disk space on the computer where Oracle is running.

By default, this Knowledge Script is configured to monitor the percentage of free disk space available to a tablespace and the percentage of disk space used by a tablespace. You can choose any combination of monitoring options and set thresholds for each one.

Resource Objects

Oracle Server icon, Oracle tablespaces icon, individual tablespace icons

Note
When run on the Oracle server icon, a single Knowledge Script job monitors every tablespace in every database on that server. When run on a tablespaces icon, a single Knowledge Script job monitors every tablespace in the database. Or you can run a Knowledge Script job on a single tablespace icon.

Default Schedule

The default interval for this script is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, this script returns statistics (percentage of free disk space or amount of disk space used) for each tablespace on which the script is running. The script returns only the data being monitored. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.

Description	How to Set It
Monitor percentage of free disk space for tablespace?	Enter **y** to monitor the percentage of disk space available to the tablespace. The default is y.
Minimum threshold for percentage of free disk space	Specify the minimum percentage of available disk space needed for the tablespace. If the amount of available space is less than this number, an event is raised. The default is 5 percent.
Monitor percentage of disk space used by tablespace?	Enter **y** to monitor the percentage of disk space used by the tablespace. The default is y.
Maximum threshold for percentage of disk space used	Specify the maximum percentage of disk space that the tablespace is allowed to use. If the percentage of disk space used by the tablespace exceeds this number, an event is raised. The default is 95%.
Monitor amount of free disk space for tablespace?	Enter **y** to monitor the amount of disk space available to the tablespace. The default is n.
Minimum threshold for amount of free disk space	Specify the minimum amount of available disk space (in MB) needed for the tablespace. If the amount of available space is less than this number, an event is raised. The default is 5 MB.
Monitor amount of disk space used?	Enter **y** to monitor the amount of disk space used by the tablespace. The default is n.
Maximum threshold for amount of disk space used	Specify the maximum amount of disk space (in MB) that the tablespace is allowed to use. If the amount of disk space used exceeds this number, an event is raised. The default is 1000 MB.
Monitor total size of tablespace?	Enter **y** if you want to monitor the total size of the tablespace. The default is n.
Maximum threshold for total size	Specify the maximum size (in MB) allowed for the tablespace. If the size of the tablespace is greater than this number, an event is raised. The default is 1024.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

TopCpuUsers

Use this Knowledge Script to monitor the CPU time for current user sessions. If the CPU usage exceeds the threshold you set, an event is raised. You can specify the number of top user sessions to display in the event and data detail messages. The detail message includes the CPU usage for each of the top *n* sessions, username, session ID, and program name.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the total CPU time for the top *N* users. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for CPU cycles (1/100 sec)	Enter a threshold for the maximum number of CPU cycles per 1/100th of a second. The default is 50 CPU cycles.
Number of user sessions to display	Specify the number of top user sessions you want displayed in the detail message (event or data). Enter 0 if you want information for all user sessions displayed. The default is 10 user sessions.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

TopIOUsers

Use this Knowledge Script to monitor physical reads and writes (I/O) for current user sessions. If the number of physical reads/writes per second exceeds the threshold you set, an event is raised. You can specify the number of top user sessions to display in the event and data detail messages. The detail message includes the physical reads/writes per second for each of the top *N* sessions, username, session ID, and program name.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the total number of physical reads/writes per second for the top *N* users. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for physical reads/writes	Enter a threshold for the maximum number of physical reads/writes per second. The default is 300 I/O operations.
Number of user sessions to display	Specify the number of top user sessions you want displayed in the detail message (event or data). Enter 0 if you want information for all user sessions displayed. The default is 10 user sessions.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

TopLockUsers

Use this Knowledge Script to monitor the current number of user-held locks on an Oracle database. If the number of locks exceeds the threshold you set, an event is raised. You can specify the number of top user sessions to display in the detail event and data messages. The detail message includes the number of locks held by each session, username, session ID, and program name.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the current number of user-held locks. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for total user locks	Enter a threshold for the maximum number of user-held locks on an Oracle server. The default is 1000 locks.
Number of user sessions to display	Specify the number of top user sessions you want displayed in the detail message (event or data). Enter 0 if you want all user sessions displayed. The default is 10 user sessions.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

TopMemoryUsers

Use this Knowledge Script to monitor memory usage (User Global Area and Program Global Area) for current user sessions. If the user memory usage exceeds the threshold you set, an event is raised. You can specify the number of top user sessions to display in the event and data detail messages. The detail message includes the memory in bytes for each session, username, session ID, and program name.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the total memory usage for the top *n* number of user sessions in MB. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for total user memory usage	Enter a threshold for the maximum memory for all user sessions in megabytes. The default is 10 MB.
Number of top memory user sessions to display	Specify the number of top user sessions you want displayed in the detail message (event or data). Enter 0 if you want information for all user sessions displayed. The default is 10 user sessions.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

TransactionRate

Use this Knowledge Script to monitor the transaction rate for an Oracle database. This Knowledge Script tracks the number of transactions per second and provides a basic measure of application workload.

Changes to your applications or to usage patterns can affect the transaction rate, but in general, an increase in the transaction rate suggests an increase in overall server load. If you observe a decrease in the transaction rate with the same number of connected users, it may indicate that you need to do some database tuning or investigate the reasons for the changes.

If the number of transactions per second exceeds the threshold you set, an event is raised.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the current transaction rate. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for transaction rate	Enter a threshold for the maximum number of transactions per second. The default is 1 transaction per second.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

UserCallsPerParse

Use this Knowledge Script to monitor the number of user calls per parse. The number of user calls per parse indicates how well an application is managing its context area. Changes in this ratio may indicate changes to the application itself or to changing usage patterns, for example, because users are moving from one module to another more or less frequently.

Generally, if the ratio is greater than or equal to 1, it indicates the SQL statements are executing efficiently without frequent reparsing. If the ratio is less than 1, it indicates the private SQL area may be too small.

When the ratio of user calls (parse, execute, fetch) to total parse calls falls below the threshold you set, an event is raised.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a Knowledge Script monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the current user calls per parse ratio. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Minimum threshold for user calls per parse	Enter a threshold for the minimum number of user calls per parse. The default is 1 call per parse.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

UserRollbackRatio

Use this Knowledge Script to monitor the user rollback ratio for an Oracle Database server. The user rollback ratio indicates the percentage of attempted application transactions that fail. The ratio compares the number of transactions rolled back to the total number of transactions attempted.

Because rolling back a transaction uses significant system resources, an increase in this ratio suggests resources have been wasted in attempting to execute failed transactions. If you observe a continued increase in this ratio, it may indicate serious application or database performance problems. When the rollback ratio exceeds the threshold you set, an event is raised.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a single Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a single Knowledge Script monitors just that database.

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the current user rollback ratio. The default is n.
Username	Specify the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for user rollback ratio	Enter a threshold for the maximum percentage of transaction rollbacks that should be allowed before generating an event. The default is 75 percent.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

UserSessions

Use this Knowledge Script to monitor the total number of user sessions accessing an Oracle database. If the total number of user sessions is higher than the threshold you set, an event is raised. You can specify the number of user sessions to display in the detail event and data message. The detail message includes the number of sessions for each user and the username.

Resource Objects

Oracle Server folder, Oracle Database icon

Note
When run on the Oracle Server folder, a single Knowledge Script job monitors every database on that server. When run on a single Oracle Database icon, a single Knowledge Script monitors just that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for use in graphs and reports. When set to y, the script returns the total number of user sessions. The default is n.
Username	Specifty the Oracle username that this Knowledge Script uses to access the target databases. If you run this Knowledge Script on more than one database, each database must be configured with the same username. The default username is `system`. For more information, see "How Knowledge Scripts Access Oracle Databases" on page 3253.
Maximum threshold for total user sessions	Specify the maximum number of user sessions. The default is 100.
Number of user sessions to display	Specify the number of user sessions you want displayed in the detail message (event or data). Type *0* if you want all user sessions displayed. The default is 10.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Chapter 57
Oracle-RT Knowledge Scripts

The Oracle-RT category provides the following Knowledge Scripts for monitoring Oracle Database response time.

From the Knowledge Script view of Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ADOQuery	Queries an Oracle Database server using ADO.
AdvancedADOQuery	Queries an Oracle Database server using ADO and advanced connection parameters.
ODBCQuery	Queries an Oracle Database server using ODBC.
Report_Oracle-RT	Reports availability and response time information gathered by several Oracle-RT Knowledge Scripts.

Note
You must be able to configure a Network Service or SID in order to use the Oracle-RT Knowledge Scripts.

ADOQuery

Use this Knowledge Script to query an Oracle Database server using ADO.

Collecting Data

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to 3 response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. For more information, see "Setting Parameter Values" on page 3324.
- **Availability**–Returns one of two values:
  - 1 or 100 = transaction was successful
  - 0 = transaction was not successful.

  The Availability data point is an indication of whether the transaction succeeded or failed.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. See the description of the **Event on** parameter.

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The Oracle-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is *not* generated.
- The job transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

Resource Object

The Oracle-RT ADO client

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Be sure to set the **Integrated Security?** parameter correctly according to the security model you want to use:

- **For Oracle authentication**: Clear the **Yes** check box for the "Integrated security" parameter, then specify the Oracle Logon Username and Password parameters. Also, specify for the series of **Run As** Knowledge Script parameters a valid domain account under which to run the script.

- **Windows NT authentication** (for Oracle servers on Windows only): Select the **Yes** check box for the **Integrated security** parameter, and leave the Oracle Username and Password fields blank. The user defined in the **Run As** Knowledge Script parameters must be created as an external user at the Oracle Database server.

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect data for graphs and reports. If enabled, returns: • 1 or 100 -- Transaction completed successfully • 0 -- Transaction did not complete successfully By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Oracle used a 0 (“not available”) or 1 (“available”) format to indicate availability. You now have the option to use a 0 (“not available”) or 100 (“available”) format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, events are enabled.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5. If you disable availability failure events, this value is ignored.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect data for graphs and reports. If enabled, the system returns the time taken to complete the ADO query. By default, data is collected. If you enable data collection, you also have the option to see a breakdown in the response times for the component parts of the query, such as the time taken to connect to the Oracle server. See the **Response Time Breakdown** parameters, below.
Threshold -- Maximum response time (seconds)	Specify the maximum time, in seconds, that it can take to complete the ADO query before an event is raised. The default is 15 seconds.
Raise event when threshold is exceeded?	Select the **Yes** check box to raise an event when the response-time threshold is exceeded. By default, events are enabled.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15. If you disable response time events, this value is ignored.
Response Time Breakdown	
Collect data for connecting to Oracle server?	Select the **Yes** check box to collect response time data showing how much of the overall response time could be attributed to the time taken to establish a connection to the Oracle server. By default, breakdown data is not collected.
Collect data for executing SQL statement?	Select the **Yes** check box to collect response time data showing how much of the overall response time could be attributed to the time taken to execute the SQL statement. By default, breakdown data is not collected.

Description	How to Set It
Collect data for fetching data?	Select the **Yes** check box to collect response time data showing how much of the overall response time could be attributed to the time taken to perform a `fetch` of the query data. By default, breakdown data is not collected.
Target computer	Enter the identifier to use to enable retrieval of data streams by AppManager Analysis Center v2.0 or later. The name of the Oracle server will be used in the data stream legend, if specified. If you are setting the **Event on** parameter, the **Target computer** parameter lets you select the server where the event will appear in your console. Enter the name of the server, or click the browse button ([**...**]) to select from a list of available servers. The server you select must already be in the TreeView.
Network Service Name	Enter the Network Service Name or SID configured on the client.
Provider	Select the OLEDB Provider to use for the ADO connection. The following drivers are supported: **Microsoft**=Microsoft OLEDB Provider for Oracle (installed with MDAC). This is the default. **Oracle**=Oracle Provider for OLEDB (provided by Oracle).
Cursor location	Enter the location of the cursor service: • `CLIENT`: Uses client-side cursors supplied by a local cursor library. Local services may allow many features not allowed by driver-supplied cursors; using this setting may provide some advantage in enabling features. • `SERVER`: Uses data provider- or driver-supplied cursors. These cursors may be flexible and allow for additional sensitivity to changes made to the data source by others. This is the default.
SQL statement	Enter a SQL statement (1024-character maximum) that is compatible with the provider.
Number of rows per fetch	Enter any positive integer or -1. Use an appropriate value according to the size of the result and of a single row. Default value is 1. If the SQL statement is a select, the engine uses the `GetRows()` method to retrieve the data, so you can fetch thousands of records at once. This could mean a huge performance improvement in production. A value of -1 attempts to retrieve all rows on a single fetch. Although this may show interesting results on a small database, it can easily become catastrophic if the result is large and the client computer has limited memory. You should change this value only if the `GetRows()` method is used in production with a value different than 1.
Integrated security?	Select the **Yes** check box to specify whether the authentication should be done on the Windows NT integrated security model. By default, authentication is not performed. **Note**: This parameter is only supported with Oracle Database running on Windows.

Description	How to Set It
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** The client computer in the response-time tests. This is the default. • **Server** The Oracle Database server being tested--see the **Target computer** parameter, above • **Both**. The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Oracle Logon	
Username	Set this value when you do *not* use integrated security. This is the User ID part of the Connection Properties collection.
Password	Set this value when you do *not* use integrated security. This is the Password part of the Connection Properties collection. Hard encryption is always used.
Run As	
Username	Enter the user ID associated with a specific user who has the required permissions to run this application. This value is also used for Integrated Security. Interactive User is also a possible value. Leave the **Password** and **Domain** parameters blank if you specify “Interactive User”.
Password	Enter the password associated with this user that is required to log on to the network and run the application.
Domain	Enter the domain associated with this user that is the domain name you are logging onto.
Administrators group on managed client	Enter the name of the Administrators Group on the managed client. Typically, this name is “`Administrators`”, except on some foreign-language operating systems. The default is “`Administrators`”.
Timeouts	
Command timeout	Enter the number of seconds to wait while executing a command before terminating the attempt and generating an error. Default is 30 seconds.
Connection timeout	Enter the number of seconds to wait while establishing a connection before terminating the attempt and generating an error. Default is 15 seconds.

AdvancedADOQuery

Use this Knowledge Script to check the ability to query an Oracle Database server query using ADO and advanced connection parameters.

Collecting Data

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to 3 response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. For more information, see "Setting Parameter Values" on page 3324.
- **Availability**–Returns one of two values:
  - 1 or 100 = transaction was successful
  - 0 = transaction was not successful.

  The Availability data point is an indication of whether the transaction succeeded or failed.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. See the description of the **Event on** parameter, below.

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The Oracle-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is *not* generated.
- The job transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

Resource Object

The Oracle-RT ADO client

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Be sure to set the **Integrated Security?** parameter correctly, according to the security model you want to use:

- **For Oracle authentication**: Clear the **Yes** check box for the **Integrated security** parameter, then specify the Oracle Username and Password. Also, specify valid account information for the **Run As** Knowledge Script parameters. The Knowledge Script must have a valid domain account to run.

- **For Windows NT authentication** (for Oracle Database servers on Windows only): Select the **Yes** check box for the **Integrated security** parameter, and leave the Oracle Username and Password fields blank. The user defined in the **Run As** parameters must be created as an external user at the Oracle Database server.

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect data for graphs and reports. If enabled, returns: • 1 or 100 -- Transaction completed successfully • 0 -- Transaction did not complete successfully By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Oracle used a 0 (“not available”) or 1 (“available”) format to indicate availability. You now have the option to use a 0 (“not available”) or 100 (“available”) format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, an event is raised.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5. If you disable availability failure events, this value is ignored.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect data for graphs and reports. If enabled, returns the time taken to complete the ADO query. By default, data is collected. If you enable data collection, you also have the option to see a breakdown in the response times for the component parts of the query, such as the time taken to connect to the Oracle server. See the **Response Time Breakdown** parameters, below.
Threshold -- Maximum response time (seconds)	Specify the maximum time, in seconds, that it can take to complete the ADO query before an event is raised. The default is 15 seconds.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the response-time threshold is exceeded. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15 (yellow event indicator).
Response Time Breakdown	
Collect data for connecting to Oracle server?	Select the **Yes** check box to collect response-time data showing how much of the overall response time could be attributed to the time taken to establish a connection to the Oracle server. By default, breakdown data is not collected.
Collect data for executing SQL statement?	Select the **Yes** check box to collect response-time data showing how much of the overall response time could be attributed to the time taken to execute the SQL statement. By default, breakdown data is not collected.
Collect data for fetching data?	Select the **Yes** check box to collect response-time data showing how much of the overall response time could be attributed to the time taken to perform a `fetch` of the query data. By default, breakdown data is not collected.

Description	How to Set It
Target computer	Enter the identifier to use to enable retrieval of data streams by AppManager Analysis Center v2.0 or later. The name of the Oracle server will be used in the data stream legend, if specified. If you are setting the **Event on** parameter, the **Target computer** parameter lets you select the server where the event will appear in your console. Enter the name of the server, or click the browse button ([**...**]) to select from a list of available servers. The server you select must already be in the TreeView.
Network Service Name	Enter the Network Service Name or SID configured on the client.
Provider	Select the OLEDB Provider to use for the ADO connection. **Microsoft**=Microsoft OLEDB Provider for Oracle (installed with MDAC). This is the default. **Oracle**=Oracle Provider for OLEDB (provided by Oracle).
Attributes	Specify the `ADODB::Connection` attributes as follows: • `NONE` (the default). No attributes. • `ABORTRETAINING`: Performs retaining aborts; i.e., calls `RollbackTrans` and automatically starts a new transaction. Not supported by all providers. • `COMMITRETAINING`: Performs retaining commits; i.e., calls CommitTrans and automatically starts a new transaction. Not supported by all providers. • `ABORTCOMITRETAINING`: A combination of `ABORTRETAINING` and `COMMITRETAINING`.
Cursor location	Enter the location of the cursor service: • `CLIENT`: Uses client-side cursors supplied by a local cursor library. Local services may allow many features not allowed by driver-supplied cursors; using this setting may provide some advantage in enabling features. • `SERVER`: Uses data provider- or driver-supplied cursors. These cursors may be flexible and allow for additional sensitivity to changes made to the data source by others. This is the default.
Isolation level	Specify the level of transaction isolation for a Connection object as follows: • `UNSPECIFIED`: Provider is using a different isolation level than specified, but that level cannot be determined. • `CHAOS`: You cannot overwrite pending changes from more highly isolated transactions. • `BROWSE`: You can view uncommitted changes in other transactions from one transaction. • `READUNCOMMITTED`: Same as `BROWSE`. • `CURSORSTABILITY`: You can view changes in other transactions from one transaction only after they have been committed. • `READCOMMITTED`: Same as `BROWSE`. This is the default. • `REPEATABLEREAD`: You cannot see changes made in other transactions from one transaction; however, requerying can retrieve new `Recordset` objects. • `ISOLATED`: Transactions are conducted in isolation from other transactions. • `SERIALIZABLE`: Same as `ISOLATED`.

Description	How to Set It
Mode	Set the available permissions for modifying data in a connection, as follows: • `UNKNOWN`: Permissions have either not yet been set or cannot be determined. This is the default. • `READ`: Read-only permissions. • `WRITE`: Write-only permissions. • `READWRITE`: Read/write permissions. • `RECURSIVE`: Not supported at this time. • `SHAREDENYNONE`: Allows others to open a connection with any permission. Neither read nor write access can be denied to others. • `SHAREDENYREAD`: Prevents others from opening a connection with read permissions. • `SHAREDENYWRITE`: Prevents others from opening a connection with write permissions. • `SHAREEXCLUSIVE`: Prevents others from opening a connection.
SQL statement	Enter a SQL statement (1024-character maximum) that is compatible with the provider.
Number of rows per fetch	Enter any positive integer or -1. Use an appropriate value according to the size of the result and of a single row. Default value is 1. If the SQL statement is a `select`, the engine uses the `GetRows()` method to retrieve the data, so you can fetch thousands or records at once. This could mean a huge performance improvement in production. A value of -1 attempts to retrieve all rows on a single fetch. Although this may show interesting results on a small database, it can easily become catastrophic if the result is large and the client machine has limited memory. You should change this value only if the `GetRows()` method is used in production with a value different than 1.
Integrated security?	Specify whether the authentication should be done on the Windows NT Integrated Security model.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** The client computer in the response-time tests. This is the default. • **Server** The Oracle Database server being tested--see the **Target computer** parameter, above. • **Both**. The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Oracle Logon	
Username	Set this value when you do *not* use Integrated Security. This is the User ID part of the Connection Properties collection.
Password	Set this value when you do *not* use Integrated Security. This is the Password part of the Connection Properties collection. Hard encryption is always used.
Run As	
Username	Enter the user ID associated with a specific user who has the required permissions to run this application. **Required**. Interactive User is also a possible value. Leave the Password and Domain parameters blank if you specify “Interactive User”.

Description	How to Set It
Password	Enter the password associated with this user that is required to log on to the network and run the application.
Domain	Enter the domain associated with this user that is the domain name you are logging onto. **Required**.
Administrators group on managed client	Enter the name of the Administrators Group on the managed client. Typically, this name is “`Administrators`”, except on some foreign language operating systems. Default is “`Administrators`”.
Timeouts	
Command timeout	Enter the number of seconds to wait while executing a command before terminating the attempt and generating an error. Default is 30 seconds.
Connection timeout	Enter the number of seconds to wait while establishing a connection before terminating the attempt and generating an error. Default is 15 seconds.

ODBCQuery

Use this Knowledge Script to query an Oracle Database server using Open Database Connectivity (ODBC) and measure the response time.

Collecting Data

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to 3 response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. For more information, see "Setting Parameter Values" on page 3324.
- **Availability**–Returns one of two values:
  - 1 or 100 = transaction was successful
  - 0 = transaction was not successful.

  The Availability data point is an indication of whether the transaction succeeded or failed.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. See the description of the **Event on** parameter, below.

An event is generated whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The Oracle-RT engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is *not* generated.
- The job transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

Resource Object

The Oracle-RT ODBC client

Default Schedule

The default schedule is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	

Description	How to Set It
Collect data for availability?	Select the **Yes** check box to collect data for graphs and reports. If enabled, returns: • 1 or 100 -- Transaction completed successfully • 0 -- Transaction did not complete successfully By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Oracle used a 0 (“not available”) or 1 (“available”) format to indicate availability. You now have the option to use a 0 (“not available”) or 100 (“available”) format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the server cannot be contacted. By default, an event is raised.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5. If you disable availability failure events, this value is ignored.
Response Time	
Collect data for response time?	Select the **Yes** check box to collect data for graphs and reports. If enabled, returns the time taken to complete the ODBC query. By default, data is collected. If you enable data collection, you also have the option to see a breakdown in the response times for the component parts of the query, such as the time taken to connect to the Oracle server. See the **Response Time Breakdown** parameters, below.
Threshold -- Maximum response time (seconds)	Specify the maximum time, in seconds, that it can take to complete the ODCBC query before an event is raised. The default is 15 seconds.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the response-time threshold is exceeded. By default, events are enabled.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15 (yellow event indicator).
Response Time Breakdown	
Collect data for connecting to Oracle server?	Select the **Yes** check box to collect response-time data showing how much of the overall response time could be attributed to the time taken to establish a connection to the Oracle server. By default, breakdown data is not collected.
Collect data for executing SQL statement?	Select the **Yes** check box to collect response-time data showing how much of the overall response time could be attributed to the time taken to execute the SQL statement. By default, breakdown data is not collected.
Collect data for fetching data?	Select the **Yes** check box to collect response-time data showing how much of the overall response time could be attributed to the time taken to perform a `fetch` of the query data. By default, breakdown data is not collected.

Description	How to Set It
Target computer	Enter the identifier to use to enable retrieval of data streams by AppManager Analysis Center v2.0 or later. The name of the Oracle server will be used in the data stream legend, if specified. If you are setting the **Event on** parameter, the **Target computer** parameter lets you select the server where the event will appear in your console. Enter the name of the server, or click the browse button ([**...**]) to select from a list of available servers. The server you select must already be in the TreeView.
Network Service Name	Enter the Network Service Name or SID configured on the client.
SQL statement	Set this value appropriately based on your DSN settings.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** The client computer in the response-time tests. This is the default. • **Server** The Oracle Database server being tested--see the **Target computer** parameter, above. • **Both**. The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Oracle Logon	
Username	Set this value appropriately based on your DSN settings.
Password	Set this value appropriately based on your DSN settings.
Run As	
Username	Enter the user ID associated with a specific user who has the required permissions to run this application. **Required**. Interactive User is a possible value. Leave the Password and Domain parameters blank if you specify “Interactive User”.
Password	Enter the password associated with this user that is required to log on to the network and run the application.
Domain	Enter the domain associated with this user that is the domain name you are logging onto.
Administrators group on managed client	Enter the name of the Administrators Group on the managed client. Typically, this name is “`Administrators`”, except on some foreign-language operating systems. Default is “`Administrators`”.
Connection timeout	Enter the number of seconds to wait while establishing a connection before terminating the attempt and generating an error. Default is 15 seconds.

Report_Oracle-RT

Use this Report Script to generate a report detailing availability and response time for the following Oracle-RT Knowledge Scripts:

- ADOQuery
- AdvancedADOQuery
- ODBCQuery

Resource Object

AppManager repository

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	Use the following parameters to select the data for your report.
KS for report	Select the Knowledge Script on which to report: 1. Click the **...** button to show the Filter KS List dialog box. 2. Select a filter to narrow the list of Knowledge Scripts and click **OK** to display the list of Knowledge Scripts that met the filter specifications. 3. If you click **Cancel** from the Filter dialog box, all the Knowledge Scripts are displayed. 4. Highlight a SQL-RT Knowledge Script from the **Knowledge Script Name** list and click **Finish**.
Oracle-RT client(s)	Select the AppManager ResponseTime for Oracle client(s). Click the **...** button to show the **Select view(s) and a filter** dialog box. From the View(s) list, select from one to twenty-five views. Your subsequent selections are limited to computers or server groups that are visible in the selected views. Select one of the Filters options: • **View:** Includes all computers in the views you selected. • **Computer:** Select from individual computers in the views you selected. • **Server Group:** Select from server groups in the views you selected. Selecting a server group includes all computers in that group.
Oracle Network Service or “All”	Type the name of the Oracle Network Service, or type “`All`” to designate all computers as Oracle Network Services. The default is “`All`”.
Select time range	In the Select Date/Time Range dialog box, set specific start and end report information dates (good for historical or ad hoc reports), or a sliding range (the default) that sets the time range of data to include in the report. This option is useful for reports running on a regular schedule and is the default.

Description	How to Set It
Select peak weekday(s)	In the Select Peak Weekday(s) dialog box, press **Shift** to select a contiguous day range, or **Ctrl** to select non-contiguous days.
Aggregation by	Select the time unit by which to aggregate data. Default is Hour. This works in conjunction with the next field **Aggregation interval**, which determines the number of units for one interval of data aggregation.
Aggregation interval	Select the interval units in which to aggregate data. Default is 1. For example, if you aggregate by the Hour and select 1 here, data is aggregated once every hour.
Report Settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter card?	Select the **Yes** check box to specify whether to display a table of parameter values used in the report.
Include Availability Detail table?	Select the **Yes** check box to specify whether to display the Availability detail table as part of the report. By default, table is included.
Availability data stream format	Specify the data stream format. Options are 0-100 or 0-1. The default format is 0-100.
Include Availability chart?	Select the **Yes** check box to display the Availability chart as part of the report. By default, chart is included.
Threshold on Availability chart	Enter an integer for the percent. Default is 0 (no threshold is displayed).
Include Response Time Detail table?	Select the **Yes** check box to specify whether to display the Response Time Detail table as part of the report. By default, the table is included.
Include Response Time chart?	Select the **Yes** check box to specify whether to display the Response Time chart as part of the report. By default, the chart is included.
Units for Response Time report	Select the response time unit of msec (the default) or sec.
Threshold on Response Time chart (selected units)	Enter the units > 0, or use the default of 0. Zero suppresses the threshold indicator in the chart.
Select chart style	Select the **...** button to display the Chart Settings dialog box where you can set the appearance of the chart. The same parameters are used in both the Availability and Response Time charts, if both are produced. The default is Ribbon.
Select output folder	Select the **...** button to display the Publishing Options dialog box. From this dialog, specify the report filename and the report folder. You can specify a specific folder or have the system generate the folder each time the report runs.
Add job ID to output folder name?	Select the **Yes** check box to add a job ID to the output folder name.
Index-Report Title	Select the **...** button to display the Report Properties dialog box. From this dialog, you can configure report title settings and custom fields.
Add timestamp to title?	Select the **Yes** check box to add a timestamp to the report title. By default, the timestamp is not included.
Event Notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Generate event on success?	Select the **Yes** check box raise an event when a report is generated. By default, events are enabled.
Severity level for report success	Set the severity level for a successful report. Default is 35.
Severity level for report with no data	Set the severity level for a report with no data. Default is 25.

Description	How to Set It
Severity level for report failure	Set the severity level for a report with no data. Default is 5.

Chapter 58
OracleUNIX Knowledge Scripts

The OracleUNIX category provides Knowledge Scripts for monitoring Oracle RDBMS.

From the Knowledge Script view of Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ActiveTransactions	Monitors the number of active transactions that are ongoing as a percentage of the maximum number of transactions that can be executed concurrently (set as an initialization parameter).
AlertLog	Scans the Oracle RDBMS alert log for entries that match a search string that you specify.
BGProc	Monitors the total memory usage and the total number of physical read/write (I/O) operations per second for Oracle RDBMS background processes.
Block	Monitors block-level database activity (visits per transaction and changes per transaction).
BlockingSessions	Monitors the user sessions that are blocking other sessions and processes from accessing the Oracle RDBMS.
BufferBusyWaits	Monitors the number of buffer busy waits and the number of logical reads, and computes a ratio between the two numbers (expressed as a percentage).
Cache	Monitors the frequency with which requested data and resources are retrieved from the cache.
CallRate	Monitors the demand placed on a database instance from all sources.
CallsPerTransaction	Monitors the demand placed on a database instance by each transaction.
ClusterInstanceDown	Monitors Oracle instances in a cluster and notifies you when an instance fails or becomes inactive.
ConsistentChangeRatio	Monitors the extent to which applications exercise the read consistency mechanism to ensure database consistency.
ContinuedRowRatio	Monitors rows that span more than one database block.
DatabaseConnect	Checks the connectivity to Oracle databases.
DatabaseDown	Monitors the status of the background processes of a database.
DataFileSpace	Monitors the size of the datafile of an Oracle RDBMS.

Knowledge Script	What It Does
DataRatios	Monitors the Consistent Change Ratio, Continued Row Ratio, Row Source Ratio, and Sort Overflow Ratio.
DiskSpaceAvail	Monitors the amount of disk space available for the archive log file, the background process log file, and user log files of a database.
FreeListWaits	Monitors the number of freelist waits and the total number of data requests, and computes a ratio of the two numbers.
HealthCheck	Monitors Oracle instances in a cluster, the connectivity to Oracle databases, and the status of the background process of Oracle database.
Listener	Monitors Oracle listeners running on the host.
Memory	Monitors the Oracle background processes, buffer busy waits, cache, and freelist waits.
MostExecutedSQLStatements	Determines which SQL statements are being executed on a given Oracle Database most frequently.
OpenCursors	Monitors the percentage of cursors opened per session, as well as the total number of cursors open in the system.
Performance	Monitors the open cursors, CPU time for current user sessions, physical reads and writes (I/O) for current user sessions, the current number of user-held locks on an Oracle Database, and memory usage (User Global Area and Program Global Area) for current user sessions.
RedoLog	Monitors the number of times that a process tries to write an entry in the redo log buffer, the number of redo logs not archived, if archiving is turned on for a given Oracle Database, and the redo log space wait ratio.
RedoLogContention	Monitors the number of times that a process tries to write an entry in the redo log buffer.
RedoLogsNotArchived	Monitors the number of redo logs which are not being archived, if archiving is turned on for a given Oracle Database.
RedoLogSpaceWaitRatio	Monitors the redo log space wait ratio.
RollbackSegmentContention	Monitors rollback segment contention for a database.
RowSourceRatio	Monitors the row source ratio.
RunSql	Runs a SQL statement.
ScheduledJobs	Monitors the scheduled job status in the New Oracle Scheduler.
SegmentExtentAvail	Monitors the percentage of extents (extensions of free space) available to each segment in a tablespace.
SetMonitoringOptions	Sets the various monitoring options available for OracleUNIX jobs, especially in clustered environments.
SortOverflowRatio	Monitors the sort overflow ratio.
SysStat	Monitors statistics from V$SYSSTAT table of an Oracle Database.
TablespaceAvail	Monitors the disk space used by tablespaces.
TopCpuUsers	Monitors the CPU time for current user sessions
TopIOUsers	Monitors physical reads and writes (I/O) for current user sessions.
TopLockUsers	Monitors the current number of user-held locks on an Oracle RDBMS.

Knowledge Script	What It Does
TopMemoryUsers	Monitors memory usage (User Global Area and Program Global Area) for current user sessions.
TopResourceConsumingSQL	Determines which SQL queries for Oracle Database are consuming the most resources per execution on their UNIX hosts.
Transaction	Monitors the number of active transactions, the demand placed on a database instance from all sources, the demand placed on a database instance by each transaction, and the transaction rate for an Oracle Database.
TransactionRate	Monitors the transaction rate for an Oracle RDBMS.
UpdateInstances	Updates the list of Oracle databases/instances on each UNIX host used to update authentication information in the AppManager Service Manager and for discovery of new databases.
User	Monitors the number of user calls per parse, the user rollback ratio for an Oracle RDBMS, the total number of user sessions accessing an Oracle RDBMS, and the user sessions that are blocking other sessions and processes from accessing the Oracle Database.
UserCallsPerParse	Monitors the number of user calls per parse.
UserRollbackRatio	Monitors the user rollback ratio for an Oracle RDBMS.
UserSessions	Monitors the total number of user sessions accessing an Oracle RDBMS.

ActiveTransactions

Use this Knowledge Script to retrieve the number of active transactions that are ongoing, and the maximum number of transactions that can be executed concurrently (set as an initialization parameter). This script computes a ratio, expressed as a percentage, of the two numbers. When you enable data collection, the percentage is stored in the repository. You can set multiple thresholds for the maximum ratio, and the job raises an event when any of the thresholds exceeds the value you specified.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$PARAMETER
V$TRANSACTION
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and collects the number of active transactions and the number of total transactions. The ratio of active transactions over total transactions is then computed.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for the ratio of active transactions to maximum concurrent transactions?	Set to **y** to collect data for charts and reports. If data collection is enabled, returns the ratio of active transactions to maximum concurrent transactions as a percentage (%). By default, data is not collected.
Raise event if ratio exceeds threshold?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job raises events.
Threshold – ratio of active transactions to max concurrent transactions	Specify a threshold for the maximum ratio of active transactions to maximum concurrent transactions, expressed as a percentage. The default for this threshold is 95%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 5 (red event indicator).
Raise event if ratio exceeds threshold?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.

Description	How to Set It
Threshold – ratio of active transactions to max concurrent transactions	Specify a threshold for the maximum ratio of active transactions to maximum concurrent transactions, expressed as a percentage. The default for this threshold is 80%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 15 (yellow event indicator).
Raise event if ratio exceeds threshold?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- ratio of active transactions to max concurrent transactions	Specify a threshold for the maximum ratio of active transactions to maximum concurrent transactions, expressed as a percentage. The default for this threshold is 60%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 25 (blue event indicator).
Raise event if ratio exceeds threshold?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- ratio of active transactions to max concurrent transactions	Specify a threshold for the maximum ratio of active transactions to maximum concurrent transactions, expressed as a percentage. The default value is 40%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 35 (magenta event indicator).

AlertLog

Use this Knowledge Script to scan the Oracle alert log for entries that match a specified search string. You can set a maximum threshold for the number of occurrences of the string found during any single scan of the alert log. If during any single scan of the alert log the number of matching entries exceeds the threshold, the job raises an event.

Each database maintains an alert log where it records database operations (such as creating or dropping a database) and error conditions (such as deadlocks). This script provides a general-purpose tool for scanning a database's alert log for specific entries.

The first interval of this script does not scan existing entries, and does not collect data. Instead, it sets a pointer to the end of the alert log so that only new entries are read. Each subsequent iteration of the script scans the alert log for entries created since the previous scan. Information in the Event Properties dialog box states the number of occurrences of the search string that were found. The lines containing matches found in the log are also included in the event details.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$PARAMETER
V$VERSION
```

Notes

When the Oracle alert log reaches its maximum size, Oracle renames the file for archiving purposes and creates a new alert log with the original filename. If this script attempts to open the alert log between the time the old file is renamed and the new file is created, the job raises an event because the script cannot find the file. The next iteration of the script (when the alert log is available) should function as expected.

This script attempts to open the alert log associated with the relevant Oracle instance. Oracle instance alert logs use the naming convention alert_<instance name>.

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for number of matching log entries?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the number of entries that matched the search string. By default, data is not collected.
String(s) to find in log (separate multiple strings with semicolons)	Enter all or part of the strings you want to find in the log. For this script, a string is any series of characters (including spaces, if doing an exact match search). You can specify multiple strings by separating each string with a semicolon (;). For example, if you specify `ORA-600;ORA-1578` the script searches for either of two strings: `ORA-600` or `ORA-1578`. The default values represent the most common Oracle error codes: • `ORA-600` (internal error) • `ORA-1578` (block corruption) • `ORA-60` (deadlock error)
Optional file with string(s) to find in log (one search string per line)	Specify the full path to a file that contains strings to search for in the alert log (one search string per line). If a path is specified, the strings specified in the previous parameter (**String(s) to find in log**) are ignored. By default, no path is specified.
Search Options	
Execute a case-sensitive search?	Set to **y** to find only case-sensitive matches of the search string. By default, the search is not case-sensitive.
Find only entries that exactly match?	Set to **y** to find only entries that match the exact search string character-for-character and whole word-for whole word. For example, a search for "`ORA-60″` will not return a match for "`ORA-600″`. By default, only exact matches are found.
Raise event if threshold exceeded?	Select the **Yes** check box to raise an event when the number of log entries found that match the search criteria exceeds the threshold you set. By default, events are enabled.
Threshold -- Maximum number of entries found	Enter a threshold for the maximum number of log entries that can be found to match the search criteria during any single scan of the alert log. If the number of entries matches or exceeds the threshold, the job raises an event. The default value is 0 entries.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

BGProc

Use this Knowledge Script to monitor the total number of physical read/write (I/O) operations per second and/or the total memory usage for Oracle RDBMS background processes. If the total number of read/write operations per second or the total memory usage exceeds the threshold, the job raises an event.

Oracle background processes include `CKPT`, `DBW0`, `LGWR`, `PMON`, `RECO`, `SMON`, `SNP0`, and others. You can monitor all or individual background processes.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$BGPROCESS
V$PROCESS
V$SESSION
V$SESSTAT
V$STATNAME
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target Oracle RDBMSs. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for memory usage and I/O of Oracle processes?	Set to **y** to collect data for charts and reports. If data collection is enabled, returns the number of read/write operations per second, and/or the total memory usage for all monitored background processes. By default, data is not collected.

Description	How to Set It
Oracle background processes to monitor	Enter the names of the background processes you want to monitor. Separate the names with commas; do not use spaces. To monitor all Oracle RDBMS background processes, enter an asterisk (*). Possible valid background process names include: • CKPT • DBW0 • LGWR • PMON • RECO • SMON • SNP0 • SNP1 The default value is (*) (all background processes).
Monitor read/write operations?	Select the **Yes** check box to monitor the number of physical read/write operations per second by background processes. By default, monitoring is performed.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the number of physical read/write operations per second exceeds the threshold you set. By default, events are not enabled.
Threshold -- Maximum number of read/write operations	Enter a threshold for the maximum number of physical read/write operations per second. The default value is 5 read/write operations per second.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15 (yellow event indicator).
Monitor memory usage?	Select the **Yes** check box to monitor the total memory usage by background processes. By default, monitoring is performed.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the memory utilization of the monitored processes exceeds the threshold you set. By default, events are not enabled.
Threshold -- Maximum memory usage	Enter a threshold (in MB) for the maximum amount of memory used by all background processes you are monitoring. The default value is 15 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15 (yellow event indicator).

Block

Use this Knowledge Script to monitor block-level database activity. Oracle RDBMS data blocks are the smallest unit of storage for a database. Monitoring I/O activity at the block level can be a key indicator of database performance.

Use this script to monitor any combination of the following statistics:

- The number of block changes per transaction. This **block change rate** measures the number of SQL Data Manipulation Language (DML) commands that each transaction performs (for example, to create and drop indexes). As the number of block changes increases, the efficiency of the database transaction and database performance decreases.
- The number of times the Oracle RDBMS buffer manager locates a database per second. This **block get rate** indicates the rate at which an application references the database. An increase in the block get rate suggests an increase in overall server load. A decrease in the block get rate without a decrease in load may indicate that you need to do some database tuning because there has been a slowdown in the number of database blocks requested and located per second.
- The number of times database blocks are requested per committed transaction. This **block visit rate** measures the database work load per completed transaction (including both successful and aborted database transactions).

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for block activity?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the statistics you choose to collect: • The number of block changes per transaction • The number of block `get` operations per second • The number of block visits per transaction By default, data is not collected.

Description	How to Set It
Monitor block change rate?	Select the **Yes** check box to monitor the block change rate, the number of block changes per transaction. By default, monitoring is performed.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the block change rate exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum block change rate	Enter a threshold for the maximum number of block changes per transaction before the job raises an event. The default value is 100 changes per transaction.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).
Monitor block get rate?	Select the **Yes** check box to monitor the block get rate, the number of times the Oracle RDBMS buffer manager locates a database block per second. By default, monitoring is performed.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the block get rate exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum block get rate	Enter a threshold for the maximum number of block get operations per second before the job raises an event. The default value is 100 get operations per second.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).
Monitor block visit rate?	Select the **Yes** check box to monitor the block visit rate, the number of times database blocks are requested per committed transaction. By default, monitoring is performed.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the block visit rate exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum block visit rate	Enter a threshold for the block visit rate, the maximum number of block get operations per committed transaction. The default value is 100 operations per committed transaction.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

BlockingSessions

Use this Knowledge Script to monitor the user sessions that are blocking other sessions and processes from accessing the Oracle Database. You can set a maximum threshold for the number of sessions that are allowed to block other sessions and processes. If the number of blocking sessions exceeds the threshold, the job raises an event.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$LOCK
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for number of blocking sessions?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the number of blocking sessions per interval. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the number of blocking sessions exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum number of blocking sessions	Enter a threshold for the maximum number of user sessions allowed to block other user sessions and processes during the monitoring interval. The default value is 10 sessions.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

BufferBusyWaits

Use this Knowledge Script to retrieve the number of buffer busy waits and the number of logical reads, and compute a ratio between the two numbers (expressed as a percentage). When you enable data collection, the repository stores the ratio. You can set multiple thresholds for the maximum ratio, and the job raises an event when any of the thresholds exceeds the value you specified. A higher ratio indicates an increased contention for buffers in the SGA memory of Oracle Database.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSTEM_EVENT
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and collects the number of buffer busy waits and the number of logical reads. The ratio of buffer waits over logical reads is then computed.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for ratio of buffer busy waits to logical reads?	Set to **y** to collect data for charts and reports. If data collection is enabled, returns the ratio of buffer busy waits to logical reads as a percentage (%). By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, events are enabled.
Threshold -- Maximum ratio of buffer busy waits to logical reads	Specify a threshold for the maximum ratio of buffer busy waits to logical reads. The default for this threshold is.95.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 5 (red event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the ratio exceeds the threshold specified below. By default, the job does not raise events.
Threshold –- Maximum ratio of buffer busy waits to logical reads	Specify a threshold for the maximum ratio of buffer busy waits to logical reads. The default value is .80.

Description	How to Set It
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 15 (yellow event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold –- Maximum ratio of buffer busy waits to logical reads	Specify a threshold for the maximum ratio of buffer busy waits to logical reads. The default value is .60.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 25 (blue event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold –- Maximum ratio of buffer busy waits to logical reads	Specify a threshold for the maximum ratio of buffer busy waits to logical reads. The default value is .40.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 35 (magenta event indicator).

Cache

Use this Knowledge Script to monitor the frequency with which requested data and resources are retrieved from the cache. As this hit ratio (that is, the percentage of time that data or resources are retrieved from the cache) decreases, performance also decreases because data that must be retrieved from disk or library objects must be reinitialized in order to service the requests.

Use this script to monitor any combination of the following statistics:

- The *buffer cache hit ratio* indicates the percentage of time that requested data you can find in the buffer cache.
- The *data dictionary hit ratio* indicates the percentage of time that requested data you can find in the data dictionary.
- The *library cache hit ratio* indicates the percentage of time that the system requests to access objects in the library cache and you can service without re-initializing or reloading library objects. Changes to the library cache hit ratio may occur when an application becomes active, causing more SQL statements and stored procedures to be used.

You can set a threshold for each cache hit ratio you choose to monitor. If a cache hit ratio falls below a threshold you set, the job raises an event.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$LIBRARYCACHE
V$ROWCACHE
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for monitored metrics?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the statistics you choose to collect: • The buffer cache hit ratio • The data dictionary hit ratio • The library cache hit ratio By default, data is not collected.

Description	How to Set It
Monitor buffer cache hit ratio?	Select the **Yes** check box to monitor the percentage of time that requested data you can find in the buffer cache. By default, monitoring is performed.
Raise event if threshold is not met?	Select the **Yes** check box to raise an event if the buffer cache hit ratio exceeds the threshold you set. By default, the job raises an event.
Threshold -- Minimum buffer cache hit ratio	Enter a minimum threshold for the buffer cache hit ratio. If the actual hit ratio falls below than this threshold, the job raises an event. Ideally, you should set this percentage relatively high because the more frequently Oracle RDBMS uses the buffer, the better your database performance. When the actual hit ratio falls below the threshold you set, the event alerts you that database performance has degraded. The default value is 70%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Monitor data dictionary hit ratio?	Select the **Yes** check box to monitor the percentage of time that requested data you can find in the data dictionary. By default, monitoring is performed.
Raise event if threshold is not met?	Select the **Yes** check box to raise an event if the data dictionary hit ratio falls below the threshold you set. By default, the job raises an event. .
Threshold -- Minimum data dictionary hit ratio	Enter a minimum threshold for the data dictionary hit ratio. If the actual hit ratio falls below this threshold, the job raises an event. Ideally you should set this percentage high because the more frequently Oracle uses the data dictionary to service requests, the better your database performance. When the actual hit ratio falls below the threshold you set, the event alerts you that database performance has deteriorated. The default value is 90%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Monitor library cache hit ratio?	Select the **Yes** check box to monitor the percentage of time that system pin requests to access objects in the library cache you can service without re-initializing or reloading library objects. By default, monitoring is performed.
Raise event if threshold is not met?	Select the **Yes** check box to raise an event if the library cache hit ratio falls below the threshold you set. By default, the job raises events.
Threshold -- Minimum library cache hit ratio	Enter a minimum threshold for the library cache hit ratio. If the actual hit ratio falls below this threshold, the job raises an event. Ideally, you should set this percentage extremely high because re-initializing or reloading library objects imposes a significant performance hit. When the actual hit ratio falls below the threshold you set, the event alerts you that database performance has degraded. The default value is 95%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).

CallRate

Use this Knowledge Script to monitor the demand placed on a database instance from all sources. This demand is determined by tracking the number of database calls per second from all applications and processes accessing the database `instance.` The database calls that are tracked include `Parse`, `Execute`, and `Fetch` statements. These calls are sometimes described as **user calls**. When the call rate (and thus the workload demand on the server) exceeds the threshold you set, the job raises an event.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for call rate?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the total user calls per second for all work sources. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the maximum number of calls per second exceeds the threshold. By default, the job raises events.
Threshold -- Maximum call rate	Enter a threshold for the maximum number of calls per second allowed before the job raises an event. The default value is 100 calls per second.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

CallsPerTransaction

Use this Knowledge Script to monitor the demand placed on a database instance by each transaction. This demand is determined by tracking the number of database calls (for example, to parse, execute, and fetch data) per committed transaction. When the number of database requests per transaction exceeds the threshold, the job raises an event.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for number of calls per transaction?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the number of database calls per transaction. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the number of calls per transaction exceeds the threshold. By default, the job raises events.
Threshold -- Maximum number of calls per transaction	Enter a threshold for the maximum number of database calls per transaction allowed before the job raises an event. The default value is 100 calls per transaction.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

ClusterInstanceDown

Use this Knowledge Script to be notified when an Oracle instance in a cluster fails or becomes inactive.

Run this Knowledge Script for Oracle RAC monitoring only. This Knowledge Script uses the `srvctl` command functionality to fetch the statuses of all the cluster instances.

The account you use to run this script must have `SELECT` permissions for the following tables:

`V$VERSION`
`GV$INSTANCE` (for Oracle RAC monitoring only)

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and determines if the instance running on that host is active or inactive.

Default Schedule

The default schedule for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	For RAC cluster monitoring, enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** This parameter must not be blank if you are deploying RAC cluster monitoring. If you are deploying non-RAC cluster monitoring, this parameter is ignored. The default value is blank.
Collect data for instance status?	Set to **y** to collect data for charts and reports. If you enable data collection, the script returns the status of each instance: • 100--instance is running • 0--instance is down By default, data is not collected.
RAC Instance Exclude Filter	Select the **Yes** check box to to exclude RAC instances.
RAC Instance to be excluded for status check [comma separated]	Enter the names of the RAC instances you want to exclude.
Raise event if instance is down or if unable to check status?	Select the **Yes** check box to raise an event when the instance is down. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event detecting that an instance is down. The default severity level is 10 (red event indicator).

ConsistentChangeRatio

Use this Knowledge Script to monitor the extent to which applications exercise the read consistency mechanism to ensure database consistency.

The consistent change ratio is based on the number of database changes and database reads. "Consistent changes" refers to the number of times a consistent `Get` had to retrieve an old version of a database block because of updates that occurred after the cursor had been opened. When the ratio of consistent changes to consistent `Gets` exceeds the threshold, the job raises an event. The ratio is recalculated each time the script runs, based on the data collected during that monitoring interval.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data **for consistent change ratio**?	Set to **y** to collect data for charts and reports. When you enable data collection, the script returns the ratio of consistent changes to consistent gets. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the consistent change ratio exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum consistent change ratio	Enter a threshold for the maximum ratio of consistent block changes to consistent block gets during the monitoring interval. The default ratio is 0.01 consistent changes/consistent gets.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

ContinuedRowRatio

Use this Knowledge Script to monitor rows that span more than one database block. This script monitors the ratio of continued rows fetched to all rows fetched.

In most cases, this ratio should be close to zero. If the continued row ratio increases over time (indicating that more and more rows span multiple database blocks), it may mean that the `PCTFREE` storage parameter is set too low for one or more tables. If the continued row ratio exceeds the threshold, the job raises an event. The ratio is recalculated each time the script runs, based on the data collected during that interval.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for continued row ratio?	Set to **y** to collect data for charts and reports. When you enable data collection, the script returns the continued row ratio. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the continued row ratio exceeds the threshold. By default, the job raises events.
Threshold -- Maximum continued row ratio (0.0 to 1.0)	Enter a threshold for the maximum ratio of continued rows fetched to all rows fetched. Enter values from 0.0 to 1.0, inclusive. The default ratio is 0.01.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

DatabaseConnect

Use this Knowledge Script to monitor the connectivity and login capability of Oracle databases on UNIX and Linux systems. This script attempts to connect to the database you select. If the connection attempt is successful, this script reports the status of the database and of its login capability. If the connection attempt is unsuccessful, an event is raised.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$INSTANCE
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for connection and login status?	Set to **y** to collect data for charts and reports. If you enable data collection, the script returns the status of the database and of its login capability. By default, data is not collected.
Raise event if unable to connect?	Select the **Yes** check box to raise an event if an attempt to connect to the Oracle database is unsuccessful. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).
Raise event with database and login status?	Select the **Yes** check box to raise an event providing information on the database and login status. By default, the job does not raise events.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 35 (magenta event indicator).

DatabaseDown

Use this Knowledge Script to monitor the status of a database. This script checks whether the Oracle background processes are running and whether a local connection can be made.

Each Oracle instance has a default set of background processes that must be running. An event is raised if any of the processes that you specified for monitoring in the **Background processes to monitor** parameter are down, or if a connection cannot be made to the database instance.

The account you use to run this script must have `SELECT` permissions for the following table:

`V$VERSION`

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for process and connection status?	Set to **y** to collect data for charts and reports. When you enable data collection, the script returns the following values: • 100--all specified processes are running and a connection attempt was successful • 80--one or more processes was down but a connection attempt was successful • 0--no processes were running and/or a connection attempt failed This provides a way to report on the percentage of system uptime in any given period. By default, data is not collected.
Background processes to monitor (comma-separated, no spaces)	Enter the names of Oracle background processes you want to monitor, separated by commas and no spaces. The default value is: `LGWR,PMON,SMON,RECO,DBWO,DBWR.`
Create blackout file for a database if it appears to be down?	Select the **Yes** check box if the script should create a file in the blackout directory so that no further jobs are run on this database. The SetMonitoringOptions script must be run to set the blackout directory before this file can be created. By default, the file is not created.

Description	How to Set It
Raise event if a process is down or unable to connect?	Select the **Yes** check box to raise an event if an Oracle database or background process is detected down. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15 (yellow event indicator).

DataFileSpace

Use this Knowledge Script to monitor the size of an Oracle datafile. When the size of the datafile (in MB) exceeds the threshold, the job raises an event.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$VERSION
V$DATAFILE
```

Resource Objects

Individual Oracle RDBMS UNIX Datafiles. When dropped on a single datafile, the script monitors only that datafile.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for datafile size?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the current size of the datafile (in MB). By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if a datafile exceeds the size threshold you set. By default, the job raises events.
Threshold -- Maximum datafile size	Enter a threshold for the maximum size a datafile can reach (in MB) before AppManager raises an event. The default value is 20 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).

DataRatios

Use this Knowledge Script to monitor the following data ratios:

- **Consistent Change Ratio**: the extent to which applications exercise the read consistency mechanism to ensure database consistency.

  The consistent change ratio is based on the number of database changes and database reads. "Consistent changes" refers to the number of times a consistent `Get` had to retrieve an old version of a database block because of updates occurring after the cursor had been opened. When the ratio of consistent changes to consistent `Gets` exceeds the threshold, the job raises an event. The ratio is recalculated each time the script runs, based on the data collected during that monitoring interval.

- **Continued Row Ratio**: the rows that span more than one database block and the ratio of continued rows fetched to all rows fetched.

  In most cases, this ratio should be close to zero. If the continued row ratio increases over time (indicating that more and more rows span multiple database blocks), it may mean that the `PCTFREE` storage parameter is set too low for one or more tables. If the continued row ratio exceeds the threshold, the job raises an event. The ratio is recalculated each time the script runs, based on the data collected during that interval.

- **Row Source Ratio**: the row source ratio for an Oracle RDBMS database. This ratio measures the percentage of rows retrieved using full table scans. Because a full table scan is less efficient than retrieval by row ID, this ratio gives you an indication of potential database performance problems. If you see an increase in this ratio, you may want to review other statistics to find the source of the problem. When this ratio exceeds the threshold, the job raises an event.

- **Sort Overflow Ratio**: the sort overflow ratio. This ratio compares the number of sorts that are using temporary segments to the total number of sorts. If the sort overflow ratio exceeds the threshold you set, the job raises an event.

  An increase in the sort overflow ratio indicates that more sort operations are allocating work space on disk. If an excessive number of sorts are allocating work space on disk, you may want to increase the sort area size.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 1Hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Ratios	
Consistent Change Ratio	Select the **Yes** check box to monitor Consistent Change Ratio.
Continued Row Ratio	Select the **Yes** check box to monitor Continued Row Ratio.
Row Source Ratio	Select the **Yes** check box to monitor Row Source Ratio.
Sort Overflow Ratio	Select the **Yes** check box to monitor Sort Overflow Ratio.
Event Notification	
Raise event if threshold is exceeded for Consistent Change Ratio?	Select the **Yes** check box to raise an event if the consistent change ratio exceeds the threshold you set. By default, the job raises events.
Raise event if threshold is exceeded for Continued Row Ratio?	Select the **Yes** check box to raise an event if the continued row ratio exceeds the threshold you set. By default, the job raises events.
Raise event if threshold is exceeded for Row Source Ratio?	Select the **Yes** check box to raise an event if the percentage of rows retrieved using a full table scan exceeds the threshold you set. By default, the job raises events.
Raise event if threshold is exceeded for Sort Overflow Ratio?	Select the **Yes** check box to raise an event if the sort overflow ratio exceeds the threshold you set. By default, the job raises events.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Data Collection	
Collect data for Consistent Change Ratio?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the script returns the ratio of consistent changes to consistent gets. By default, data is not collected.
Collect data for Continued Row Ratio?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the script returns the continued row ratio. By default, data is not collected.
Collect data for Row Source Ratio?	Select the **Yes** check box to collect data for graphs and reports. When you enable data collection, the script returns the percentage of rows retrieved using a full tables scan. By default, data is not collected.

Description	How to Set It
Collect data for Sort Overflow Ratio?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the script returns the ratio of the number of sorts using temporary segments versus the number that of sorts that are not using temporary segments. For example, a ratio of .75 indicates that 3 out of 4 sorts are using temporary segments. By default, data is not collected.
Monitoring	
Threshold -- Maximum consistent change ratio	Enter a threshold for the maximum ratio of consistent block changes to consistent block gets during the monitoring interval. The default ratio is 0.01 consistent changes/consistent gets.
Threshold -- Maximum continued row ratio [0.0 to 1.0]	Enter a threshold for the maximum ratio of continued rows fetched to all rows fetched. Enter values from 0.0 to 1.0, inclusive. The default ratio is 0.01..
Threshold -- Maximum row source ratio	Enter a maximum threshold for the row source ratio. The default ratio is .25.
Threshold -- Maximum sort overflow ratio?	Enter a threshold for the maximum sort overflow ratio allowed before the job raises an event. The default ratio is .75.

DiskSpaceAvail

Use this Knowledge Script to monitor the amount of disk space available for the archive log file, the background process log file, and user log files for a database. You can monitor the space available for all three, or for any combination of the three. For example, you could turn off monitoring for the archive log and background process log files and monitor just the disk space available for the user logs.

You can set a minimum threshold for each type of log file. If the amount of available disk space falls below any threshold, the job raises an event.

This Knowledge Script supports Automatic Storage Management (ASM).

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$ARCHIVE_DEST
V$PARAMETER
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for available disk space?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the amount of free disk space for each type of log file that you are monitoring. By default, data is not collected.
Monitor space available for the archive log?	Select the **Yes** check box to monitor the amount of disk space available for thearchive log file of the database. By default, monitoring is performed.
Raise event if threshold is not met?	Select the **Yes** check box to raise an event if space available for the archive log falls below the minimum threshold. By default, the job raises events.
Threshold -- Minimum archive log space	Enter a threshold for the minimum available disk space for the archive log file. If the available space falls below this threshold, the job raises an event. The default value is 100 MB.

Description	How to Set It
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Monitor space available for background process log?	Select the **Yes** check box to monitor the amount of space available for the background process log file of the database. By default, monitoring is performed.
Raise event if threshold is not met?	Select the **Yes** check box to raise an event if space available for the background process log file falls below the threshold. By default, the job raises events.
Threshold -- Minimum background process log space	Enter a threshold for the minimum available disk space for the background process log file. If the amount of available space falls below this threshold, the job raises an event. The default value is 100 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Monitor space available for user logs?	Select the **Yes** check box to monitor the amount of space available for the user log files of the database. By default, monitoring is performed.
Raise event if threshold is not met?	Select the **Yes** check box to raise an event if space available for the user log file falls below the threshold. By default, the job raises events.
Threshold -- Minimum user log space	Enter a threshold for the minimum available disk space for user log files. If the amount of available space falls below this threshold, the job raises an event. The default value is 100 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).

FreeListWaits

Use this Knowledge Script to retrieve the number of freelist waits and the total number of data requests, and to compute a ratio of the two numbers. You can set multiple thresholds for the ratio of freelist waits to data requests, and the job raises events when any one of the thresholds exceeds the value you specified.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
V$WAITSTAT
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and collects the number of freelist waits and the number of total data requests. The ratio of freelist waits to total data requests is then computed.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for ratio of freelist waits to total data requests?	Set to **y** to collect data for charts and reports. If data collection is enabled, returns the ratio of freelist waits to total data requests. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, events are enabled.
Threshold –- Maximum ratio of freelist waits to data requests	Specify a threshold for the maximum ratio of freelist waits to total data requests. The default for this threshold is .95.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 5 (red event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold –- Maximum ratio of freelist waits to data requests	Specify a threshold for the maximum ratio of freelist waits to total data requests. The default for this threshold is .80.

Description	How to Set It
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 15 (yellow event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold –- Maximum ratio of freelist waits to data requests	Specify a threshold for the maximum ratio of freelist waits to total data requests. The default for this threshold is .60.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 25 (blue event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold –- Maximum ratio of freelist waits to data requests	Specify a threshold for the maximum ratio of freelist waits to total data requests. The default for this threshold is .40.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 35 (magenta event indicator).

HealthCheck

Use this Knowledge Script to monitor the following parameters:

- **Cluster Instance Down**: notify when an Oracle instance in a cluster fails or becomes inactive.

  Run this Knowledge Script for Oracle RAC monitoring only. This Knowledge Script uses the `srvctl` command functionality to fetch the statuses of all the cluster instances.

- **Database Connect**: the connectivity and login capability of Oracle databases on UNIX and Linux systems. This script attempts to connect to the database you select. If the connection attempt is successful, this script reports the status of the database and of its login capability. If the connection attempt is unsuccessful, an event is raised.

- **Database Down**: the status of a database. This script checks whether the Oracle background processes are running and whether a local connection can be made.

  Each Oracle instance has a default set of background processes that must be running. An event is raised if any of the processes that you specified for monitoring in the **Background processes to monitor** parameter are down, or if a connection cannot be made to the database instance.

The account you use to run this script must have `SELECT` permissions for the following tables:

`V$INSTANCE`

`V$VERSION`
`GV$INSTANCE` (for Oracle RAC monitoring only)

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. Note To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Health Check	
Cluster Instance Down	Select the **Yes** check box to monitor Cluster Instance Down.
Database Connect	Select the **Yes** check box to monitor Database Connect.
Database Down	Select the **Yes** check box to monitor Database Down.
Data Collection	

Description	How to Set It
Collect data for instance status?	Set to **y** to collect data for charts and reports. If you enable data collection, the script returns the status of each instance: • 100--instance is running • 0--instance is down By default, data is not collected.
Collect data for connection and login status?	Set to **y** to collect data for charts and reports. If you enable data collection, the script returns the status of the database and of its login capability. By default, data is not collected.
Collect data for process and connection status?	Set to **y** to collect data for charts and reports. When you enable data collection, the script returns the following values: • 100--all specified processes are running and a connection attempt was successful • 80--one or more processes was down but a connection attempt was successful • 0--no processes were running and/or a connection attempt failed This parameter provides a way to report on the percentage of system uptime in any given period. By default, data is not collected.
Event Notification	
Raise event if instance is down or if unable to check status?	Select the **Yes** check box to raise an event when the instance is down. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event detecting that an instance is down. The default severity level is 10 (red event indicator).
Raise event if unable to connect?	Select the **Yes** check box to raise an event if an attempt to connect to the Oracle database is unsuccessful. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).
Raise event with database and login status?	Select the **Yes** check box to raise an event providing information on the database and login status. By default, the job does not raise events.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 35 (magenta event indicator).
Raise event if a process is down or unable to connect?	Select the **Yes** check box to raise an event if an Oracle database or background process is detected down. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15 (yellow event indicator).
Monitoring	

Description	How to Set It
Background processes to monitor [comma-separated, no spaces]	Enter the names of Oracle background processes you want to monitor, separated by commas and no spaces. The default value is: `LGWR,PMON,SMON,RECO,DBWO,DBWR.`
Create blackout file for a database if it appears to be down?	Select the **Yes** check box if the script should create a file in the blackout directory so that no further jobs are run on this database. The SetMonitoringOptions script must be run to set the blackout directory before this file can be created. By default, the file is not created.

Listener

Use this Knowledge Script to monitor Oracle listeners running on the host. This script can attempt to connect to each Oracle database using the service name. If the local connection attempt fails, or the service name connection attempt fails, or if an error occurs while running the job, an event is generated.

If you enable the **Restart listeners that are not running?** parameter, you have three options to specify the listeners that should be restarted. If the databases where you plan to drop the script share a single listener, you can specify the Oracle Home where the listener resides and, optionally, the name of the listener in the script itself. If the name is not specified, the job will start the default listener in that Oracle Home.

Note If you choose to have this script restart an Oracle listener that is not running, the UNIX account running the NetIQ UNIX agent must have write permissions on the `$ORACLE_HOME/network/log` folder if listener logging is enabled.

If the databases where you plan to drop the script use multiple listeners, you should specify this information in either a file that is created to identify the listeners that each `$ORACLE_SID` uses or in the default `oratab` file. If a file is created for this purpose, the path should be specified in the script, and it should have the following format:

```
$ORACLE_SID:LISTENER HOME:[LISTENER NAME]
```

where `$ORACLE_SID` is the name of the database instance, `LISTENER HOME` is the `$ORACLE_HOME` of the listener that should be restarted for this instance when no listener that can be used to connect to that instance is running, and `LISTENER NAME` is the name of this listener. It is not required to specify the name of the listener, as the default listener in the Oracle Home of the listener specified can be started, but if any text is presented in this column, it will be interpreted as a listener name.

Example: A Linux host has two `$ORACLE_HOME` directories, one of version 8.1.7 and one of version 9.2.0. This environment requires that each database use a listener of its own version. Thus, the following file is created for restarting the listeners:

```
Orasid817:/oracle/product/8.1.7
Orasid920:/oracle/product/9.2.0:lsnr_new
```

In this case, the default listener in `$ORACLE_HOME/oracle/product/8.1.7` will be restarted when a listener is not running that knows about the `Orasid817` database. For the `Orasid920` database, the `lsnr_new` listener will be started from the version 9.2.0 Oracle Home.

If the path to a file containing listener information is not specified yet you have selected for listeners to be restarted, the script will use the default `oratab` file on the host to locate listener information. When this is the case, an entry in the `$ORACLE_SID` column labeled `LSNR` must exist, and the `$ORACLE_HOME` value for this identifier will be used to restart the default listener.

Example: `/etc/oratab` file

```
#
# ORACLE_SID:$ORACLE_HOME:<N:Y>
#
Orasid817:/oracle/product/8.1.7:Y
LSNR:/oracle/product/9.2.0:N
```

In this example, the format of the `oratab` is maintained, and the third column does not specify a listener name. This is because when the `oratab` file is read for listener information, there will be no use of listener names. The default listener in the Oracle Home specified for the `LSNR` entry will always be restarted.

Note This is an easy but restrictive way to specify the listener information. You should only use this option if you are running a single listener per host, yet are dropping a single job on multiple hosts where you can specify this type of information uniformly.

The account you use to run this script must have `SELECT` permissions for the following table:

`V$VERSION`

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for success or failure of listener monitoring?	Set to **y** to collect data for charts and reports. If data collection is enabled, returns the current status of the listener process and the length of time it has been running. By default, data is not collected.
Monitor Oracle background processes?	Select the **Yes** check box to monitor Oracle background processes. By default, monitoring is enabled.
Background processes to monitor (comma-separated, no spaces)	Enter the names of Oracle background processes you want to monitor, separated by commas and no spaces. The default value is `PMON,LGWR,SMON,RECO`.
Attempt a connection using service name?	Select the **Yes** check box to attempt a connection using a service name (`tnsnames` alias). By default, the connection is not attempted.
Location of `tnsnames.ora`	Specify the directory that can be used to set the `$TNS_ADMIN` environment variable so that the `tnsnames.ora` file can be found during the connection attempt using the service name. This value can be a specific folder, or it can be relative to the `$ORACLE_HOME` for the respective database. If `$ORACLE_HOME` is specified as part of the path, the script substitutes the appropriate folder path for this variable at the time the job is executed. The default location is: `$ORACLE_HOME/network/admin`.
Service Name	Specify the service name you want to use for the connection attempt. By default, this name is usually the `$ORACLE_SID` value for the database. If `$ORACLE_SID` is specified as part of the name, the script substitutes the appropriate value for the respective database at the time the job is executed. In addition, domain names may be appended to `$ORACLE_SID` or the value specified (for example, `$ORACLE_SID.netiq.eng`). The default for this parameter is `$ORACLE_SID`.

Description	How to Set It
Number of databases per host to attempt a service connection	Select the number of databases per host for which a service connection should be attempted. Options include 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 15, 20, 50, or ALL. The default value is ALL.
Restart listeners that are not running?	Select the **Yes** check box to restart listeners or specified background process(es) that are not running. By default, listeners are not restarted.
Number of attempts to restart a given listener	If you enabled the **Restart listeners that are not running?** parameter, enter the number of times the job should attempt to restart a listener that is not running before the job raises a failure event (see the **Raise event if unable to restart a listener?** parameter below). The default value is 1.
Options for specifying listener(s) to restart	Enter values below for the following parameters if you enabled the **Restart listeners that are not running?** parameter. These parameters let you select listeners to restart if they are detected as not running.
Oracle Home of listener to restart	Enter the Oracle Home where the listener to be restarted resides. The default value is blank.
Name of listener to restart	Enter the name of the listener to restart. If you do not enter a name here, the job attempts to restart the default listener. The default value is blank.
Path to file with information on listener(s) to restart (leave blank to use oratab file)	Enter a full path and filename for a file containing the names and Oracle Homes of listeners that should be restarted if they are detected down. Use this parameter to restart multiple listeners. If you do not enter a path and filename here, the job uses the default `oratab` file for the Oracle Home listed above for the **Oracle Home of listener** parameter.
Raise event if listener or background process(es) not running?	Select the **Yes** check box to raise an event when the listener or specified background processes are not running. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).
Raise event with status of any restart attempt?	Select the **Yes** check box to raise an event giving the status of any attempts to restart listeners that are not running. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 30 (magenta event indicator).
Raise event if connection attempts fail?	Select the **Yes** check box to raise an event if the connection attempts fail. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Raise event with status if listener running and connection(s) successful?	Select the **Yes** check box to raise an event with uptime information when listener is running and the connection is successful. By default, the job does not raise events.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 40 (magenta event indicator).

Memory

Use this Knowledge Script to monitor the following parameters:

- **Freelist Waits**: retrieve the number of freelist waits and the total number of data requests, and to compute a ratio of the two numbers. You can set multiple thresholds for the ratio of freelist waits to data requests, and the job raises events when any one of the thresholds exceeds the value you specified.
- **Buffer Busy Waits**: retrieve the number of buffer busy waits and the number of logical reads, and compute a ratio between the two numbers (expressed as a percentage). When you enable data collection, the repository stores the ratio. You can set multiple thresholds for the maximum ratio, and the job raises an event when any of the thresholds exceeds the value you specified. A higher ratio indicates an increased contention for buffers in the SGA memory of Oracle database.
- **Cache**: the frequency with which requested data and resources are retrieved from the cache. As this hit ratio (that is, the percentage of time that data or resources are retrieved from the cache) decreases, performance also decreases because data that must be retrieved from disk or library objects must be reinitialized in order to service the requests.

  Use this script to monitor any combination of the following statistics:

  - The *buffer cache hit ratio* indicates the percentage of time that requested data you can find in the buffer cache.
  - The *data dictionary hit ratio* indicates the percentage of time that requested data you can find in the data dictionary.
  - The *library cache hit ratio* indicates the percentage of time that system requests to access objects in the library cache you can service without re-initializing or reloading library objects. Changes to the library cache hit ratio may occur when an application becomes active, causing more SQL statements and stored procedures to be used.

  You can set a threshold for each cache hit ratio you choose to monitor. If a cache hit ratio falls below a threshold you set, the job raises an event.
- **BGProc**: the total number of physical read/write (I/O) operations per second and/or the total memory usage for Oracle RDBMS background processes. If the total number of read/write operations per second or the total memory usage exceeds the threshold, the job raises an event.

  Oracle background processes include `CKPT`, `DBW0`, `LGWR`, `PMON`, `RECO`, `SMON`, `SNP0`, and others. You can monitor all or individual background processes.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
V$WAITSTAT

V$LIBRARYCACHE
V$ROWCACHE
V$SYSTEM_EVENT

V$BGPROCESS
V$PROCESS
V$SESSION
V$SESSTAT
V$STATNAME
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Memory	
Freelist Waits	Select the **Yes** check box to monitor the Freelist Waits.
Buffer busy Waits	Select the **Yes** check box to monitor the Buffer Busy Waits.
Cache	
Monitor buffer cache hit ratio?	Select the **Yes** check box to monitor the percentage of time that requested data you can find in the buffer cache. By default, monitoring is performed.
Monitor data dictionary hit ratio?	Select the **Yes** check box to monitor the percentage of time that requested data you can find in the data dictionary. By default, monitoring is performed.
Monitor library cache hit ratio?	Select the **Yes** check box to monitor the percentage of time that system pin requests to access objects in the library cache you can service without re-initializing or reloading library objects. By default, monitoring is performed.
BGProc	
Oracle background porcesses to monitor	Enter the names of the background processes you want to monitor. Separate the names with commas; do not use spaces. To monitor all Oracle RDBMS background processes, enter an asterisk (*). Possible valid background process names include: • CKPT • DBW0 • LGWR • PMON • RECO • SMON • SNP0 • SNP1 The default value is (*) (all background processes).
Monitor read/write operations?	Select the **Yes** check box to monitor the number of physical read/write operations per second by background processes. By default, monitoring is performed.

Description	How to Set It
Monitor memory usage?	Select the **Yes** check box to monitor the total memory usage by background processes. By default, monitoring is performed.
Event Notification	
Raise event if threshold is exceeded for ratio of freelist waits to total data requests?	
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, events are enabled.
Threshold -- Maximum ratio of freelist waits to data requests	Specify a threshold for the maximum ratio of freelist waits to total data requests. The default for this threshold is .95.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 5 (red event indicator).
Raise event if ratio exceeds threshold?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- Maximum ratio of freelist waits to data requests	Specify a threshold for the maximum ratio of freelist waits to total data requests. The default for this threshold is .80.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 15 (yellow event indicator).
Raise event if ratio exceeds threshold?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- Maximum ratio of freelist waits to data requests	Specify a threshold for the maximum ratio of freelist waits to total data requests. The default for this threshold is .60.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 25 (blue event indicator).
Raise event if ratio exceeds threshold?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- Maximum ratio of freelist waits to data requests	Specify a threshold for the maximum ratio of freelist waits to total data requests. The default for this threshold is .40.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 35 (magenta event indicator).
Raise event if threshold is exceeded for ratio of buffer busy waits to logical reads?	
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the specified limit. By default, events are enabled.
Threshold -- Maximum ratio of buffer busy waits to logical reads	Specify a threshold for the maximum ratio of buffer busy waits to logical reads. The default for this threshold is.95.

Description	How to Set It
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 5 (red event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the ratio exceeds the threshold specified below. By default, the job does not raise events.
Threshold -- Maximum ratio of buffer busy waits to logical reads	Specify a threshold for the maximum ratio of buffer busy waits to logical reads. The default value is.80.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 15 (yellow event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- Maximum ratio of buffer busy waits to logical reads	Specify a threshold for the maximum ratio of buffer busy waits to logical reads. The default value is.60.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 25 (blue event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- Maximum ratio of buffer busy waits to logical reads	Specify a threshold for the maximum ratio of buffer busy waits to logical reads. The default value is .40.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 35 (magenta event indicator).
Raise event for cache?	
Raise event if threshold is not met?	Select the **Yes** check box to raise an event if the buffer cache hit ratio exceeds the threshold you set. By default, the job raises an event.
Threshold -- Minimum buffer cache ratio	Enter a minimum threshold for the buffer cache hit ratio. If the actual hit ratio falls below than this threshold, the job raises an event. Ideally, you should set this percentage relatively high because the more frequently Oracle RDBMS uses the buffer, the better your database performance. When the actual hit ratio falls below the threshold you set, the event alerts you that database performance has degraded. The default value is 70%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Raise event if threshold is not met?	Select the **Yes** check box to raise an event if the data dictionary hit ratio falls below the threshold you set. By default, the job raises an event. .

Description	How to Set It
Threshold -- Minimum data dictionary hit ratio	Enter a minimum threshold for the data dictionary hit ratio. If the actual hit ratio falls below this threshold, the job raises an event. Ideally you should set this percentage high because the more frequently Oracle uses the data dictionary to service requests, the better your database performance. When the actual hit ratio falls below the threshold you set, the event alerts you that database performance has deteriorated. The default value is 90%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Raise event if threshold is not met?	Select the **Yes** check box to raise an event if the library cache hit ratio falls below the threshold you set. By default, the job raises events.
Threshold -- Minimum library cache hit ratio	Enter a minimum threshold for the library cache hit ratio. If the actual hit ratio falls below this threshold, the job raises an event. Ideally,you should set this percentage extremely high because re-initializing or reloading library objects imposes a significant performance hit. When the actual hit ratio falls below the threshold you set, the event alerts you that database performance has degraded. The default value is 95%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Raise event for Oracle Background processes?	
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the number of physical read/write operations per second exceeds the threshold you set. By default, events are not enabled.
Threshold -- Maximum read/write operations rate	Enter a threshold for the maximum number of physical read/write operations per second. The default value is 5 read/write operations per second.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15 (yellow event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the memory utilization of the monitored processes exceeds the threshold you set. By default, events are not enabled.
Threshold -- Maximum memory usage	Enter a threshold (in MB) for the maximum amount of memory used by all background processes you are monitoring. The default value is 15 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15 (yellow event indicator).

Description	How to Set It
Data Collection	
Collect data for ratio of freelist waits to total data requests?	Select the **Yes** check box to collect data for charts and reports. If data collection is enabled, returns the ratio of freelist waits to total data requests. By default, data is not collected.
Collect data for ratio of buffer busy waits to logical reads?	Select the **Yes** check box to collect data for charts and reports. If data collection is enabled, returns the ratio of buffer busy waits to logical reads as a percentage (%). By default, data is not collected.
Collect data for Cache?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the statistics you choose to collect: • The buffer cache hit ratio • The data dictionary hit ratio • The library cache hit ratio By default, data is not collected.
Collect data for memory usage and I/O of Oracle processes?	Select the **Yes** check box to collect data for charts and reports. If data collection is enabled, returns the number of read/write operations per second, and/or the total memory usage for all monitored background processes. By default, data is not collected.

MostExecutedSQLStatements

Use this Knowledge Script to determine which SQL queries or statements are being executed on a given Oracle database most frequently. This script identifies the *N* most frequently executed queries and returns the results in an event. You set a value for *N* using the **Number of SQL statements to retrieve** parameter.

When you enable data collection, the most frequently executed SQL statements are stored in the repository.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SQLAREA
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and collects the *N* most executed SQL statements or queries.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for most executed SQL statements?	Set to **y** to collect data for charts and reports. If data collection is enabled, returns the top *N* most frequently executed SQL statements. Set a value for *N* using the **Number of SQL statements to retrieve** parameter (see below). By default, data is not collected.
Number of SQL statements to retrieve	The number of most frequently executed SQL queries to be retrieved by the job. The default value is 10. The maximum is 30.
Raise event if error occurs during retrieval?	Select the **Yes** check box to raise an event if an error occurs during the retrieval of SQL statements. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 10 (red event indicator).

Description	How to Set It
Raise event with results from query?	Select the **Yes** check box to raise an event with details of the query results. By default, the job does not raise events.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 40 magenta event indicator).

OpenCursors

Use this Knowledge Script to monitor the percentage of cursors opened per session, as well as the total number of cursors open in the system. In the Oracle environment, a *cursor* is a type of handle (or pointer) used to identify a query in the system. Cursors can be opened by users or by the system itself. A high number of open cursors can be caused by a programming error, and may cause database performance problems. In the `init.ora` file, you can specify the maximum number of cursors that may be opened by a session.

In this script, you can specify a maximum threshold for the percentage of open cursors allowed per session--a percentage of the number specified for the `open_cursor` parameter in the `init.ora` file. For example, if the `init.ora` file specifies that 60 cursors may be open in a session, and you set a maximum threshold of 75%, the script raises an event when 75% of the 60 allowed cursors (or 45 cursors) are open in any session.

You can also specify a maximum threshold for the total number of open cursors allowed in the system. The job raises an event if either threshold exceeds the value you specified.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$PARAMETER
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for number of open cursors?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the total number of open cursors in the system. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the number of cursors open in the system exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum number of open cursors in system	Specify a maximum threshold for the number of cursors that may be open in the system. The default value is 1000 open cursors.

Description	How to Set It
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the percentage of cursors opened per session exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum percentage of cursors opened per session	Specify a maximum threshold for the percentage of open cursors per session. Note that this percentage is based on the number of open cursors allowed per session specified in the `init.ora` file. The default value is 80%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).

Performance

Use this Knowledge Script to monitor the following parameters:

- **Top CPU Users**: the CPU time for current user sessions. If the CPU utilization exceeds the threshold, the job raises an event.

  You can specify the number of user sessions with the highest CPU utilization to display in the Event Properties dialog box. The Event Properties dialog box includes the CPU usage for each of the top *N* sessions, username, session ID, and program name. Enter 0 to display all user sessions.

  This script requires that the Oracle `timed_statistics` parameter be turned on (set to `TRUE`) for the database you are monitoring.

- **Top IO Users**: physical reads and writes (I/O) for current user sessions. If the number of physical reads/writes per second (the physical read/write operations rate) exceeds the threshold you set, the job raises an event.

  You can specify the number of user sessions with the highest physical read/write operations rate to display in the Event Properties dialog box. Information in the Event Properties dialog box includes the physical reads/writes per second for each of the top *N* sessions, username, session ID, and program name.

  This script requires that the Oracle `timed_statistics` parameter is turned on for the database you are monitoring.

- **Top Lock Users**: the current number of user-held locks on an Oracle database. If the number of locks exceeds the threshold, the job raises an event.

  You can specify the number of user sessions holding the most locks to display in the Event Properties dialog box, or enter 0 to display all sessions. Information in the Event Properties dialog box includes the number of locks held by each session, username, session ID, and program name.

- **Top Memory Users**: memory utilization (User Global Area and Program Global Area) for current user sessions. If the memory utilization exceeds the threshold, the job raises an event.

  You can specify the number of user sessions with the highest memory usage to display in the Event Properties dialog box. Information in the Event Properties dialog box includes the memory in bytes for each session, username, session ID, and program name. Enter 0 for the **Number of top user sessions to display** parameter if you want to include memory utilization statistics for all user sessions in the event details.

- **Open Cursors:** the percentage of cursors opened per session, as well as the total number of cursors open in the system. In the Oracle environment, a *cursor* is a type of handle (or pointer) used to identify a query in the system. Cursors can be opened by users or by the system itself. A high number of open cursors can be caused by a programming error, and may cause database performance problems. In the `init.ora` file, you can specify the maximum number of cursors that may be opened by a session.

  In this script, you can specify a maximum threshold for the percentage of open cursors allowed per session–a percentage of the number specified for the `open_cursor` parameter in the `init.ora` file. For example, if the `init.ora` file specifies that 60 cursors may be open in a session, and you set a maximum threshold of 75%, the script raises an event when 75% of the 60 allowed cursors (or 45 cursors) are open in any session.

  You can also specify a maximum threshold for the total number of open cursors allowed in the system. The job raises an event if either threshold exceeds the value you specified.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
DBA_USERS
V$SESSION
V$SESSTAT
V$STATNAME
V$VERSION

V$LOCK

V$PARAMETER
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Performance	
Top CPU Users	Select the **Yes** check box to monitor the Top CPU Users.
Top IO Users	Select the **Yes** check box to monitor the Top IO Users.
Top Lock Users	Select the **Yes** check box to monitor the Top Lock Users.
Top Memory Users	Select the **Yes** check box to monitor the Top Memory Users.
Open Cursors	Select the **Yes** check box to monitor the Open Cursors.
Event Notification	
Raise event if threshold exceeded for Top CPU Users?	Select the **Yes** check box to raise an event if the CPU usage of any user session exceeds the threshold you set. By default, the job raises events.
Raise event if threshold exceeded for Top IO Users?	Select the **Yes** check box to raise an event if the physical read/write operations of any single user session exceed the threshold you set. By default, the job raises events.
Raise event if threshold exceeded for Top Lock Users?	Select the **Yes** check box to raise an event if the number of user-held locks on the server exceeds the threshold you set. By default, the job raises events.
Raise event if threshold exceeded for Top Memory Users?	Select the **Yes** check box to raise an event if the total memory usage of any user session exceeds the threshold you set. By default, the job raises events.

Description	How to Set It
Raise event if threshold is exceeded for Total Number of Open Cursors in the System?	Select the **Yes** check box to raise an event if the number of cursors open in the system exceeds the threshold you set. By default, the job raises events.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Raise event if threshold is exceeded for Percentage of Cursors Opened per Session?	Select the **Yes** check box to raise an event if the percentage of cursors opened per session exceeds the threshold you set. By default, the job raises events.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).
Data Collection	
Collect data for Top CPU Users?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the total CPU time for the top *N* users. By default, data is not collected.
Collect data for Top IO Users?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the total number of physical reads/writes per second for the top *N* users. By default, data is not collected.
Collect data for Top Lock Users?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the current number of user-held locks by the user sessions with the highest number of locks. By default, data is not collected.
Collect data for Top Memory Users?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the total memory usage (in MB) for the top *N* user sessions. By default, data is not collected.
Collect data for Open Cursor?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the total number of open cursors in the system. By default, data is not collected.
Monitoring	
Number of user sessions of display [Not Applicable to Open Cursor Counters]	Specify the number of user sessions you want displayed in the Event Properties dialog box. Enter **0** if you want information for all user sessions. The default value is 15 user sessions.
Threshold -- Maximum amount of CPU time for a user session	Enter a threshold for the maximum number of CPU cycles per 1/100th of a second that a single user session can use before the job raises an event. The default value is 50 CPU cycles per 1/100th of a second.
Threshold -- Maximum read/write operations for a user session	Enter a threshold for the maximum number of physical reads/writes per second allowed before the job raises an event. The default value is 300 read/write operations.

Description	How to Set It
Threshold -- Maximum number of locks held by a user session	Enter a threshold for the maximum number of user-held locks on an Oracle RDBMS. The default value is 35 locks.
Threshold -- Maximum amount of memory for a user session	Enter a threshold for the maximum total memory usage (in MB) for any user session. The default value is 10 MB.
Threshold -- Maximum percentage of cursors opened per session	Specify a maximum threshold for the percentage of open cursors per session. Note that this percentage is based on the number of open cursors allowed per session specified in the `init.ora` file. The default value is 80%.
Threshold -- Maximum number of open cursors in system	Specify a maximum threshold for the number of cursors that may be open in the system. The default value is 1000 open cursors.

RedoLog

Use this Knowledge Script to monitor the following parameters:

- **Redo Log Contention**: the number of times that a process tries to write an entry in the redo log buffer. The job raises an event and than stores data if the number of tries is different for subsequent iterations of the script.

  The number of retries should be low. A high number of retries can adversely affect system performance, as processes must wait for buffers. If a process has to make numerous attempts to write an entry in the redo log buffer, you may need to allocate more space to the redo log buffer.

  You can set a threshold value for the maximum number of times a process can try to write an entry in the redo log buffer. If the number of retries exceeds the threshold, an event is raised.

- **Redo Log Space Wait Ratio**: the redo log space wait ratio. The redo log space wait ratio measures memory allocation. The ratio reflects the number of times the background process was requested to allocate space within the redo file per number of redo log entries. If this ratio increases, you may want to increase the size of the redo log buffer.

  When the redo log space wait ratio exceeds the threshold you set, the job raises an event.

- **Redo Logs Not Archived**: retrieve the number of redo logs that are not being archived, if archiving is turned on for a given Oracle database. The number of redo logs not archived is returned and compared against the thresholds you specify. The Knowledge Script retrieves the archive status for an Oracle database from the AppManager repository, which is updated during discovery. To enable archiving, you must rediscover the Oracle UNIX resources if the redo log archive is enabled after you discover resources.

  When you enable data collection, the number of redo logs not archived is stored in the repository. You can set multiple thresholds for the number of redo logs not archived, with varying severities, and the job raises an event when any of these thresholds exceeds the value you specified.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SGASTAT
V$SYSSTAT
V$VERSION

V$LOG
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Redo Log	
Redo Log Contention	Select the **Yes** check box to monitor Redo Log Contention.
Redo Log Space wait Ratio	Select the **Yes** check box to monitor Redo Log Space Wait Ratio.
Redo Log Not Archived	Select the **Yes** check box to monitor Redo Log Not Archived.
Event Notification	
Raise event if threshold is exceeded for Redo Log Contention?	Select the **Yes** check box to raise an event if the number of times that a process tries to rewrite an entry to the redo log buffer exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum redo log buffer allocation retries	Enter a threshold for the maximum number of times that a process may try to rewrite an entry to the redo log buffer before the job raises an event. The default value is 50 retries.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).
Raise event if threshold is exceeded for Redo Log Space Wait Ratio?	Select the **Yes** check box to raise an event if the redo log space wait ratio exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum redo log space wait ratio	Enter a maximum threshold for the redo log space wait ratio. The default ratio is 0.0002.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Raise event if threshold is exceeded for Redo Logs not archived?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, events are enabled.
Threshold -- Maximum number of redo logs not archived	Specify a threshold for the maximum number of redo logs that have not been archived. The default value is 6 redo logs.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).
Raise event if threshold is exceeded for Redo Logs not archived?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- Maximum number of redo logs not archived	Specify a threshold for the maximum number of redo logs that have not been archived. The default for this threshold is 4 redo logs.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 15 (yellow event indicator).

Description	How to Set It
Raise event if threshold is exceeded for Redo Logs not archived?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- Maximum number of redo logs not archived	Specify a threshold for the maximum number of redo logs that have not been archived. The default for this threshold is 2 redo logs.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 25 (blue event indicator).
Raise event if threshold is exceeded for Redo Logs not archived?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- Maximum number of redo logs not archived	Specify a threshold for the maximum number of redo logs that have not been archived. The default for this threshold is 1 redo log.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 35 (magenta event indicator).
Data Collection	
Collect data for Redo Log Contention?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the number of times that processes attempted to write entries to the redo log buffer. By default, data is not collected.
Collect data for Redo Log Space Wait Ratio?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the redo log space wait ratio. By default, data is not collected.
Collect data for Redo Log not archived?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the number of redo logs not archived. By default, data is not collected.

RedoLogContention

Use this Knowledge Script to monitor the number of times that a process tries to write an entry in the redo log buffer for a scheduled interval of time. The job raises an event and than stores data if the number of tries is different for subsequent iterations of the script.

The number of retries should be low. A high number of retries can adversely affect system performance, as processes must wait for buffers. If a process has to make numerous attempts to write an entry in the redo log buffer, you may need to allocate more space to the redo log buffer.

You can set a threshold value for the maximum number of times a process can try to write an entry in the redo log buffer. If the number of retries exceeds the threshold, the job raises an event.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SGASTAT
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for redo log write attempts?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the number of times that processes attempted to write entries to the redo log buffer. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the number of times that a process tries to rewrite an entry to the redo log buffer exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum number of redo log buffer allocation retries	Enter a threshold for the maximum number of times that a process may try to rewrite an entry to the redo log buffer before the job raises an event. The default value is 50 retries.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

RedoLogsNotArchived

Use this Knowledge Script to retrieve the number of redo logs that are not being archived, if archiving is turned on for a given Oracle database. The number of redo logs not archived is returned and compared against the thresholds you specify. The Knowledge Script retrieves the archive status for an Oracle database from the AppManager repository, which is updated during discovery. To enable archiving, you must rediscover the Oracle UNIX resources if the redo log archive is enabled after you discover resources.

When you enable data collection, the number of redo logs not archived is stored in the repository. You can set multiple thresholds for the number of redo logs not archived, with varying severities, and the job raises an event when any of these thresholds exceed the values you specified.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$LOG
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and checks for `ARCHIVING` log mode before proceeding to monitor that database. The job then collects the number of redo logs that have not been archived. This data is collected and stored in the repository if you have enabled data collection.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for number of redo logs not archived?	Set to **y** to collect data. If data collection is enabled, returns the number of redo logs not archived. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, events are enabled.
Threshold -- Maximum number of redo logs not archived	Specify a threshold for the maximum number of redo logs that have not been archived. The default value is 6 redo logs.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

Description	How to Set It
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- Maximum number of redo logs not archived	Specify a threshold for the maximum number of redo logs that have not been archived. The default for this threshold is 4 redo logs.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 15 (yellow event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- Maximum number of redo logs not archived	Specify a threshold for the maximum number of redo logs that have not been archived. The default for this threshold is 2 redo logs.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 25 (blue event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold -- Maximum number of redo logs not archived	Specify a threshold for the maximum number of redo logs that have not been archived. The default for this threshold is 1 redo log.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 35 (magenta event indicator).

RedoLogSpaceWaitRatio

Use this Knowledge Script to monitor the redo log space wait ratio. The redo log space wait ratio measures memory allocation. The ratio reflects the number of times the background process was requested to allocate space within the redo file per number of redo log entries. If this ratio increases, you may want to increase the size of the redo log buffer.

When the redo log space wait ratio exceeds the threshold you set, the job raises an event.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for redo log space wait ratio?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the redo log space wait ratio. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the redo log space wait ratio exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum redo log space wait ratio	Enter a maximum threshold for the redo log space wait ratio. The default ratio is 0.0002.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).

RollbackSegmentContention

Use this Knowledge Script to monitor rollback segment contention for a database. In the Oracle environment, the **rollback segment** is a temporary location where changes are stored until the user makes the changes permanent. This script compares the number of requests waiting to access data from the rollback segment to the total number of requests for data during the monitoring interval.

You can specify the maximum percentage of requests allowed to wait for data from the rollback segment. If the percentage of waiting requests exceeds the threshold you set, the job raises an event. Such an event probably indicates that too many processes are waiting to access the rollback segment, in which case, you may need to create additional rollback segments.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
V$WAITSTAT
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for rollback segment contention?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the percentage of requests waiting to access the rollback segment. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the percentage of total requests that are waiting to access the rollback segment exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum percentage of requests waiting for access	Enter the maximum percentage of total requests that can be waiting to access data from the rollback segment before the job raises an event. The default value is 1%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).

RowSourceRatio

Use this Knowledge Script to monitor the row source ratio for an Oracle RDBMS. This ratio measures the percentage of rows retrieved using full table scans. Because a full table scan is less efficient than retrieval by row ID, this ratio gives you an indication of potential database performance problems. If you see an increase in this ratio, you may want to review other statistics to find the source of the problem. When this ratio exceeds the threshold, the job raises an event.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for row source ratio?	Set to **y** to collect data for use in graphs and reports. When you enable data collection, the script returns the percentage of rows retrieved using a full table scan. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the percentage of rows retrieved using a full table scan exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum row source ratio	Enter a maximum threshold for the row source ratio. The default ratio is .25.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

RunSql

Use this Knowledge Script to run a SQL statement. The statement can be entered directly in the script or loaded from a file. You specify the column to monitor, by number or name, and whether to monitor the value found in the column or the value's rate of change (changes per second). You can also specify a string that the script can search for in the retrieved rows.

This script is designed to execute simple SQL statements, for example, a statement that returns the size of a table or the number of columns in a table. There is a limit of 10000 characters for the entire statement when it is contained in a file, and a limit of 1000 characters when the statement is entered via the **SQL statement** parameter. Regardless of the source of the SQL statement, there is a limit of 100 columns retrieved by a `SELECT` statement, and a limit of 8 KB for the size of each row retrieved.

This script supports SQL statements using the `number`, `character`, `date`, and `raw` data types. However, only a column returning numeric data can be selected to monitor.

The account you use to run this script must have `SELECT` permissions for the following table:

`V$VERSION`
(plus any table the script is run against)

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data specified in the SQL query?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the number of rows returned from the SQL statement. If you choose to monitor the column's rate of change and set this parameter to y, the script returns the change in the number of rows since the last time the SQL statement was run. By default, data is collected.
Legend	Enter a legend for the output of your SQL statement. The default value is blank. If you leave this parameter blank, AppManager constructs a legend based on the column number. For example, if the column number is 0, the constructed legend is "# Result Rows". If the column number is greater than 0, the constructed legend is the specified column heading. If no heading exists, the constructed legend is: "Column <num> Value".

Description	How to Set It
Load SQL script from file?	Select the **Yes** check box to load a SQL script from a file. By default, this parameter is disabled.
SQL script file (full path)	If you set the **Load SQL script from file?** parameter to Yes, enter the complete path to the file that contains the SQL statement. For example: `/netiq/Sample.sql.`
SQL statement	If you set the **Load SQL script from file?** parameter to no, enter the SQL statement to be executed. The default statement selects all processes from the V$PROCESS table: `SELECT * FROM V$PROCESS` **Tip** Unless you are entering very simple queries, you may find typing a SQL statement into this field is error-prone. To avoid errors, use the **Load SQL script from file?** parameter. Or, if you have an AppManager Developer's license, you can check this script out of the repository, use the Knowledge Script Editor to paste the desired SQL statement into the **SQL statement** parameter, then check in the modified script.
Select column by number, or name?	Set to `Number` or `Name`: • `Number`--to select the column by number • `Name--`to select the column by name.
Column number to retrieve	If you set the **Select column by number or name?** parameter to `Number`, enter the column number to use as the primary output value. The column you specify must contain numeric data. Entering 0 returns the number of rows returned from the SQL statement. Any other positive value returns the value for the specified column's first row of data. If the specified column is not a numeric field, the job raises an event. The default value is 1.
Column name to retrieve	If you set the **Select column by number or name?** parameter to `Name`, enter the column name to use as the primary output value. The column you specify must contain numeric data. The value for the specified column's first row of data is returned. If the specified column is not a numeric field, the job raises an event.. The default value is blank.
Number of rows to display	Enter the number of rows you want displayed in the Event Properties dialog box. The default value is 5 rows. **Note:** You can enter 0 to indicate no limit (keep all output rows). Currently, however, the message in the Event Properties dialog box is limited to 32K characters.
Monitor the column's value or rate of change?	Set to `Value` to monitor the column's value. Set to `Change` to monitor the column's rate of change (per second). The default value is `Value`.
Raise event when threshold is exceeded or not met?	Select the **Yes** check box to raise an event when a threshold is crossed. By default, the job does not raise events.
Condition: <, =, or >	Indicate the condition (less than, equal to, or greater than) you want to check for. This parameter is used in conjunction with the **Threshold -- Value or rate of change** parameter to control when the job raises events. The default value is > , indicating that the job raises an event if the value retrieved exceeds (is greater than) the value specified in the threshold.

Description	How to Set It
Threshold -- Value or rate of change	Enter a threshold for the value or rate you are monitoring. Depending on how you set the **Monitor the column's value or rate of change?** parameter, this may indicate a threshold for the statistic's value or for the number of times the value changes per second. The value you set here is used in conjunction with the **Condition: <, =, or >** parameter to control when the job raises events. The default value is 1,000.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).
Raise event for string found in row results?	Select the **Yes** check box to raise an event if the string you specify below you can find in the row results. By default, the job does not raise events.
String(s) to find in results (separate multiple strings with semicolons)	Enter a string (text) to search for in row results. If you enter multiple strings, separate them with semicolons (;) and no spaces. The default value is blank.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15 (yellow event indicator).

ScheduledJobs

Use this Knowledge Script to monitor the scheduled job status in the New Oracle Scheduler. When the scheduled job fails, the job raises an event.

The account you use to run this script must have `SELECT` permissions for the following tables:

`dba_jobs`

`dba_scheduler_jobs`
(use the New Oracle Scheduler with Oracle RDBMS 10g Release 1 and later.)

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for Oracle Scheduled Jobs?	Set to **y** to collect data for Oracle scheduled jobs. When there are no failed jobs, the data value is 0. By default, data is not collected.
Include Jobs Scheduled with New Oracle Scheduler?	Select the **Yes** check box to include jobs scheduled with the New Oracle Scheduler. **Note**: You can use the New Oracle Scheduler with Oracle RDBMS 10g Release 1 and later. By default, this parameter is disabled.
Raise event if Jobs Failed?	Select the **Yes** check box to raise an event when the scheduled jobs fail. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

SegmentExtentAvail

Use this Knowledge Script to monitor either the percentage or number of extents (extensions of free space) available to each segment in a tablespace. Use the **Minimum percentage of extents available per segment** or **Minimum number of extents available per segment** parameter to define how many available extents a monitored segment should have.

You can then set multiple threshold values for the minimum number or percentage of extents that should be available for each segment. For example, you may want each segment to have at least 1,400 or 70% of extents available. You can set thresholds for the maximum number of segments that can fall below this value before the job raises an event.

In the above example, if you specify that 70% of extents should be available for each segment, and that 4 segments should be the maximum number allowed to have less than 70% of their extents available, then if 4 segments are found to have less than 70% of their extents available, the job raises an event.

Note The job raises an event only when *both* conditions are met. In the example described above, this script would not raise an event until 4 segments were found that had less than 70% of their extents available.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
DBA_SEGMENTS
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for number of segments with too few available extents?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the number of segments with less than the specified percentage or number of extents available. By default, data is not collected.
Units for available extents per segment	Set to **Percentage** to monitor the percentage of available extents per segment. Set to **Number** to monitor the number of available extents per segment. The default value is Percentage.

Description	How to Set It
Minimum percentage of extents available per segment	Enter the minimum percentage of extents that should be available for each segment in a tablespace. This parameter is used when you have selected "`Percentage`" for the **Units for available extents per segment** parameter (see above). The default value is 80%.
Minimum number of extents available per segment	Enter the minimum number of extents that should be available for each segment in a tablespace. This parameter is used when you have selected "`Number`" for the **Units for available extents per segment** parameter (see above). The default value is 10 extents.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the number of extents that fail to meet the minimum value you set for available extents within a tablespace exceeds the maximum threshold (see below). By default, events are enabled.
Threshold -- Maximum number of segments with too few extents available	Enter a threshold for the maximum number of segments whose number or percentage of available extents failed to meet the minimum requirement specified above. If the number of segments not meeting this requirement exceeds this threshold, the job raises an event. The default value is 0 segments.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 35 (magenta event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the number of extents that fail to meet the minimum value you set for available extents within a tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum number of segments with too few extents available	Enter a threshold for the maximum number of segments whose number or percentage of available extents failed to meet the minimum requirement specified above. If the number of segments not meeting this requirement exceeds this threshold, the job raises an event. The default value is 5 segments.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 25 (blue event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the number of extents that fail to meet the minimum value you set for available extents within a tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum number of segments with too few extents available	Enter a threshold for the maximum number of segments whose number or percentage of available extents failed to meet the minimum requirement specified above. If the number of segments not meeting this requirement exceeds this threshold, the job raises an event. The default value is 10 segments.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 15 (yellow event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the number of extents that fail to meet the minimum value you set for available extents within a tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.

Description	How to Set It
Threshold -- Number of segments with too few extents available	Enter a threshold for the maximum number of segments whose number or percentage of available extents failed to meet the minimum requirement specified above. If the number of segments not meeting this requirement exceeds this threshold, the job raises an event. The default value is 50 segments.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

SetMonitoringOptions

Use this Knowledge Script to set the various monitoring options available with AppManager for Oracle UNIX/Linux. You can set the location where files reside whose filenames contain the names of databases to be "blacked out" (not monitored) while they are down due to scheduled activities such as maintenance. Enter a full path to a directory containing filenames whose names indicate which databases to exclude from OracleUNIX jobs.

To reset this script, you can enable one or more parameters but leave their values blank and then run the job. For example, if you enable the **Set option for blackout monitoring?** parameter but leave the next parameter, **Full path to directory with database names to exclude**, blank, the next time you run the job, you overwrite the previous value with a blank value. This is the recommended way to reset the blackout monitoring option or any of the clustering options.

This script also lets you specify whether to monitor tablespaces with temporary contents, and/or those with autoextensible datafiles.

Note Use this script to specify monitoring options for running jobs in a clustered environment. AppManager for Oracle UNIX/Linux supports monitoring both RAC and non-RAC clustered environments.

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Set option for blackout monitoring?	Select the **Yes** check box if you should set blackout location upon executing this job iteration. By default, this parameter is disabled.
Full path to directory with database names to exclude	Specify the directory where files reside whose filenames include database names for databases that should not be monitored (databases to "black out"). The default value is blank (no databases blacked out).
Set option for monitoring temporary tablespaces?	Select the **Yes** check box if you should set the option for monitoring tablespaces with temporary contents upon executing this job iteration. By default, this option is not set.
Monitor temporary tablespaces?	Select the **Yes** check box to monitor those tablespaces with temporary contents. Clear the box to skip monitoring such tablespaces. By default, monitoring is performed.
Set option for monitoring autoextensible tablespaces?	Select the **Yes** check box if you should set the option for monitoring tablespaces with autoextensible datafiles upon executing this job iteration. By default, this option is not set.

Description	How to Set It
Monitor tablespaces with autoextensible datafiles?	Select the **Yes** check box to monitor those tablespaces with datafiles that autoextend. Clear the box to skip monitoring such tablespaces. By default, monitoring is performed.
Set option for monitoring Oracle RAC?	Select the **Yes** check box if you should set the option for monitoring computers running Oracle RAC upon executing this job iteration. By default, this option is not set.
Service name for the RAC cluster	Enter the service name identifying the Oracle RAC environment upon which the job will run. This allows the Oracle UNIX/Linux managed object to connect to Oracle on the host and determine which nodes are active. The parameter is blank by default.
Directory containing `tnsnames.ora` file (if not in default location)	Enter the path to the folder containing the `tnsnames.ora` file. This is normally what the `$TNS_ADMIN` environment variable is set to for Oracle to resolve service names. The default location is normally: `$ORACLE_HOME/network admin`. This parameter is blank by default. **Note** The default location is used if a directory is not specified here.
Set option for monitoring non-RAC cluster?	Select the **Yes** check box if you should set the option for monitoring computers running as part of a cluster where Oracle RAC is not installed upon executing this job. By default, this option is not set.
Path to a required available resource	Enter the path to a resource (file, directory, device, etc.) that must be available to the computer running the Oracle UNIX/Linux managed object in order for jobs to execute successfully. This can be a resource that a node in a cluster requires in order for that node to have access to Oracle. This parameter is blank by default.
Raise event if unable to set monitoring options?	Select the **Yes** check box to raise an event when the monitoring options could not be set. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 15 (yellow event indicator).
Raise event to display options currently set?	Select the **Yes** check box to raise an event providing a summary of the current settings for monitoring options. By default, the job does not raise events.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 40 (magenta event indicator).

SortOverflowRatio

Use this Knowledge Script to monitor the sort overflow ratio. This ratio compares the number of sorts that are using temporary segments to the total number of sorts. If the sort overflow ratio exceeds the threshold you set, the job raises an event.

An increase in the sort overflow ratio indicates that more sort operations are allocating work space on disk. If an excessive number of sorts are allocating work space on disk, you may want to increase the sort area size.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for sort overflow ratio?	Set to **y** to collect data for charts and reports. When you enable data collection, the script returns the ratio of the number of sorts using temporary segments versus the number that do not. For example, a ratio of .75 indicates that 3 out of 4 sorts are using temporary segments. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the sort overflow ratio exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum sort overflow ratio	Enter a threshold for the maximum sort overflow ratio allowed before the job raises an event. The default ratio is .75.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).

SysStat

Use this Knowledge Script to monitor statistics from a database's V$SYSSTAT table. This table stores all the key statistics for a database. You specify the statistic to monitor, and the value and condition (greater than, less than, or equal to) to check. If the **value** or **change rate** (changes per second) of a monitored statistic crosses a threshold, the job raises an event.

The account you use to run this script must have SELECT permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for a V$SYSSTAT statistic?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the current value of the specified statistic at each interval. By default, data is not collected.
V$SYSSTAT statistic to monitor	Enter the name of the statistic you want to monitor--for example, USER CALLS. For information about the fields in the V$SYSSTAT table, see your Oracle RDBMS documentation (for example, in the Oracle8 Reference, see "Appendix C: Statistics Descriptions"). The default statistic is EXECUTE COUNT.
Monitor change rate, or value of statistic?	When you select Change rate, the script monitors the number of times the value of the monitored statistic changes per second. When you select Value, the script monitors the value of the statistic. The default value is Change rate.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the threshold you set is crossed. By default, the job raises events.
Condition: <, =, or >	Indicate the condition (less than, equal to, or greater than) you want to check. This parameter is used in conjunction with the **Threshold -- Change rate or value** parameter to control when the job raises an event. The default value is > (greater than).

Description	How to Set It
Threshold -- Change rate or value	Enter a threshold value or rate for the specified statistic. Depending on how you set the **Monitor change rate or value of statistic?** parameter, this may indicate a threshold for the value of the statistic or for the number of changes in that value per second. The value you set here is used in conjunction with the **Condition: <, =, or >** parameter to control when the job raises an event. The default value is 100.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

TablespaceAvail

Use this Knowledge Script to monitor the disk space used by Oracle tablespaces.

This script can monitor the following:

- The amount of free disk space available for a tablespace (as a percentage, absolute amount, or both)
- The amount of disk space used by a tablespace (as a percentage, absolute amount, or both)
- The size of a tablespace

This script monitors only the disk space allocated to an Oracle database, not the total disk space on the computer where Oracle is running.

By default, this script is set to monitor the percentage of free disk space available to a tablespace and the percentage of disk space used by a tablespace. You can choose any combination of monitoring options and set multiple thresholds for each one.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
DBA_DATA_FILES
DBA_FREE_SPACE
DBA_TABLESPACES
DBA_TEMP_FILES
V$SORT_SEGMENT
V$VERSION
```

Resource Objects

Individual Oracle RDBMS UNIX Tablespace icons. When run on an individual tablespace, the Knowledge Script job monitors only that tablespace.

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for amount of disk space used and free, and total tablespace size?	Set to **y** to collect data for charts and reports. When you enable data collection, and if monitoring of each metric is enabled, the Knowledge Script returns the following statistics for each tablespace on which the script is running: • percentage of disk space free within the tablespace • percentage of disk space used within the tablespace • amount of disk space free within the tablespace • amount of disk space used within the tablespace • total size of tablespace By default, data is not collected.

Description	How to Set It
Absolute path of the file containing comma separated information related to tablespaces to be excluded	Enter the absolute path of the file containing information related to tablespaces that you want to exclude from raising events. Specifiy the required values in the following token entries: • 1 - name of the tablespace. • 2 - the threshold value for percentage of free space within the tablespace from which you can raise events. • 3 - the threshold value for percentage of used space within the tablespace from which you can raise events. • 4 - the threshold value for amount of free space within the tablespace from which you can raise events. • 5 - the threshold value for amount of used space within the tablespace from which you can raise events. • 6 - the threshold value for total size of the tablespace from which you can raise events. For example: system, 95, 10, 100,,3000 **Note:** If you do not want to specify a threshold value for a particular token, leave it empty as noted in the preceding example.
Monitor percentage of free space within tablespace?	Select the **Yes** check box to monitor free space as a percentage. Expand this parameter to see threshold and severity parameters. By default, monitoring is enabled.
Raise event if threshold is not met?	Select the **Yes** check box to raise an event when the percentage of free disk space within a tablespace fails to meet the minimum threshold (see below). By default, events are enabled.
Threshold -- Minimum percentage of free space	Enter a threshold for the minimum percentage of free disk space within the tablespace that must be found to prevent an event from being raised. The default value is 5%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).
Raise event if threshold is not met?	Select the **Yes** check box to raise an event when the percentage of free disk space within a tablespace fails to meet the minimum threshold (see below). By default, the job does not raise events.
Threshold -- Minimum percentage of free space	Enter a threshold for the minimum percentage of free disk space within the tablespace that must be found to prevent an event from being raised. The default value is 20%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 15 (yellow event indicator).
Raise event if threshold is not met?	Select the **Yes** check box to raise an event when the percentage of free disk space within a tablespace fails to meet the minimum threshold (see below). By default, the job does not raise events.
Threshold -- Minimum percentage of free space	Enter a threshold for the minimum percentage of free disk space within the tablespace that must be found to prevent an event from being raised. The default value is 40%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 25 (blue event indicator).

Description	How to Set It
Raise event if threshold is not met?	Select the **Yes** check box to raise an event when the percentage of free disk space within a tablespace fails to meet the minimum threshold (see below). By default, the job does not raise events.
Threshold -- Minimum percentage of free space	Enter a threshold for the minimum percentage of free disk space within the tablespace that must be found to prevent an event from being raised. The default value is 60%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 35 (magenta event indicator).
Monitor percentage of space used within tablespace?	Select the **Yes** check box to monitor used disk space as a percentage. Expand this parameter to see threshold and severity parameters. By default, monitoring is not performed.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the percentage of used disk space within a tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum percentage of space used	Enter a threshold for the maximum percentage of disk space that the tablespace can use. If the percentage of used disk space exceeds this threshold, the job raises an event. The default value is 95%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the percentage of used disk space within a tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum percentage of space used	Enter a threshold for the maximum percentage of disk space that the tablespace can use. If the percentage of used disk space exceeds this threshold, the job raises an event. The default value is 80%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 15 (yellow event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the percentage of used disk space within a tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum percentage of space used	Enter a threshold for the maximum percentage of disk space that the tablespace can use. If the percentage of used disk space exceeds this threshold, the job raises an event. The default value is 60%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 25 (blue event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the percentage of used disk space within a tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.

Description	How to Set It
Threshold -- Maximum percentage of space used	Enter a threshold for the maximum percentage of disk space that the tablespace can use. If the percentage of used disk space exceeds this threshold, the job raises an event. The default value is 40%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 35 (magenta event indicator).
Monitor amount of free space within tablespace?	Select the **Yes** check box to monitor free space as an amount, in MB. Expand this parameter to see threshold and severity parameters. By default, monitoring is not performed.
Raise event if threshold is not met?	Select the **Yes** check box to raise an event when the percentage of free disk space within a tablespace fails to meet the minimum threshold (see below). By default, the job does not raise events.
Threshold -- Minimum amount of free space	Enter a threshold for the minimum amount of free disk space within the tablespace that must be found to prevent an event from being raised. The default value is 50 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).
Raise event if threshold is not met?	Select the **Yes** check box to raise an event when the percentage of free disk space within a tablespace fails to meet the minimum threshold (see below). By default, the job does not raise events.
Threshold -- Minimum amount of free space	Enter a threshold for the minimum amount of free disk space within the tablespace that must be found to prevent an event from being raised. The default value is 100 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 15 (yellow event indicator).
Raise event if threshold is not met?	Select the **Yes** check box to raise an event when the percentage of free disk space within a tablespace fails to meet the minimum threshold (see below). By default, the job does not raise events.
Threshold -- Minimum amount of free space	Enter a threshold for the minimum amount of free disk space within the tablespace that must be found to prevent an event from being raised. The default value is 200 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 25 (blue event indicator).
Raise event if threshold is not met?	Select the **Yes** check box to raise an event when the percentage of free disk space within a tablespace fails to meet the minimum threshold (see below). By default, the job does not raise events.
Threshold -- Minimum amount of free space	Enter a threshold for the minimum amount of free disk space within the tablespace that must be found to prevent an event from being raised. The default value is 500 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 35 (magenta event indicator).

Description	How to Set It
Monitor amount of space used within tablespace?	Select the **Yes** check box to monitor used disk space as an amount, in MB. Expand this parameter to see threshold and severity parameters. By default, monitoring is not performed.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the amount of used disk space within a tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum amount of space used	Enter a threshold for the maximum amount of disk space that the tablespace can use. If the amount of used disk space exceeds this threshold, the job raises an event. The default value is 1000 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the amount of used disk space within a tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum amount of space used	Enter a threshold for the maximum amount of disk space that the tablespace can use. If the amount of used disk space exceeds this threshold, the job raises an event. The default value is 400 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 15 (yellow event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the amount of used disk space within a tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum amount of space used	Enter a threshold for the maximum amount of disk space that the tablespace can use. If the amount of used disk space exceeds this threshold, the job raises an event. The default value is 200 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 25 (blue event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the amount of used disk space within a tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum amount of space used	Enter a threshold for the maximum amount of disk space that the tablespace can use. If the amount of used disk space exceeds this threshold, the job raises an event. The default value is 100 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 35 (magenta event indicator).
Monitor total size of tablespace?	Select the **Yes** check box to monitor the total size, in MB, of the tablespace. Expand this parameter to see threshold and severity parameters. By default, monitoring is not performed.

Description	How to Set It
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the total size of the tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum total size of tablespace	Enter a threshold for the maximum size (in MB) that the tablespace can reach. If the size of the tablespace exceeds this threshold, the job raises an event. The default value is 2000 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the total size of the tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum total size of tablespace	Enter a threshold for the maximum size (in MB) that the tablespace can reach. If the size of the tablespace exceeds this threshold, the job raises an event. The default value is 800 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 15 (yellow event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the total size of the tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum total size of tablespace	Enter a threshold for the maximum size (in MB) that the tablespace can reach. If the size of the tablespace exceeds this threshold, the job raises an event. The default value is 400 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 25 (blue event indicator).
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the total size of the tablespace exceeds the maximum threshold (see below). By default, the job does not raise events.
Threshold -- Maximum total size of tablespace	Enter a threshold for the maximum size (in MB) that the tablespace can reach. If the size of the tablespace exceeds this threshold, the job raises an event. The default value is 200 MB.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 35 (magenta event indicator).

TopCpuUsers

Use this Knowledge Script to monitor the CPU time for current user sessions. If the CPU utilization exceeds the threshold, the job raises an event.

You can specify the number of user sessions with the highest CPU utilization to display in the Event Properties dialog box. The Event Properties dialog box includes the CPU usage for each of the top *N* sessions, username, session ID, and program name. Enter 0 to display all user sessions.

This script requires that the Oracle `timed_statistics` parameter be turned on (set to `TRUE`) for the database you are monitoring.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
DBA_USERS
V$SESSION
V$SESSTAT
V$STATNAME
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for CPU usage of top N user sessions?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the total CPU time for the top *N* users. By default, data is not collected.
Number of user sessions to display	Specify the number of user sessions you want displayed in the Event Properties dialog box. Enter **0** if you want information for all user sessions. The default value is 15 user sessions.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the CPU usage of any user session exceeds the threshold you set. By default, the job raises events.

Description	How to Set It
Threshold -- Maximum amount of CPU time for a user session	Enter a threshold for the maximum number of CPU cycles per 1/100th of a second that a single user session can use before the job raises an event. The default value is 50 CPU cycles per 1/100th of a second.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

TopIOUsers

Use this Knowledge Script to monitor physical reads and writes (I/O) for current user sessions. If the number of physical reads/writes per second (the physical read/write operations rate) exceeds the threshold you set, the job raises an event.

You can specify the number of user sessions with the highest physical read/write operations rate to display in the Event Properties dialog box. Information in the Event Properties dialog box includes the physical reads/writes per second for each of the top *N* sessions, username, session ID, and program name.

This script requires that the Oracle `timed_statistics` parameter is turned on for the database you are monitoring.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
DBA_USERS
V$SESSION
V$SESSTAT
V$STATNAME
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for I/O activity of top N user sessions?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the total number of physical reads/writes per second for the top *N* users. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the physical read/write operations of any single user session exceed the threshold you set. By default, the job raises events.
Threshold -- Maximum physical read/write operations for a user session	Enter a threshold for the maximum number of physical reads/writes per second allowed before the job raises an event. The default value is 300 read/write operations.

Description	How to Set It
Number of user sessions to display	Specify the number of top user sessions you want displayed in the Event Properties dialog box. Enter 0 if you want to see information for all user sessions. The default value is 10 user sessions.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

TopLockUsers

Use this Knowledge Script to monitor the current number of user-held locks on an Oracle database. If the number of locks exceeds the threshold, the job raises an event.

You can specify the number of user sessions holding the most locks to display in the Event Properties dialog box, or enter 0 to display all sessions. Information in the Event Properties dialog box includes the number of locks held by each session, username, session ID, and program name.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
DBA_USERS
V$LOCK
V$SESSION
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for locks held by top N user sessions?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the current number of user-held locks by the user sessions with the highest number of locks. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the number of user-held locks on the server exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum number of locks held by a user session	Enter a threshold for the maximum number of user-held locks on an Oracle RDBMS. The default value is 35 locks.
Number of user sessions to display	Specify the number of user sessions with the most locks that you want displayed in the Event Properties dialog box. Enter 0 if you want all user sessions displayed. The default value is 10.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

TopMemoryUsers

Use this Knowledge Script to monitor memory utilization (User Global Area and Program Global Area) for current user sessions. If the memory utilization exceeds the threshold, the job raises an event.

You can specify the number of user sessions with the highest memory usage to display in the Event Properties dialog box. Information in the Event Properties dialog box includes the memory in bytes for each session, username, session ID, and program name. Enter 0 for the **Number of top user sessions to display** parameter if you want to include memory utilization statistics for all user sessions in the event details.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
DBA_USERS
V$SESSION
V$SESSTAT
V$STATNAME
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for memory used by top N user sessions?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the total memory usage (in MB) for the top *N* user sessions. You determine how many sessions are included in this total by setting the **Number of top user sessions to display** parameter. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the total memory usage of any user session exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum amount of memory for a user session	Enter a threshold for the maximum total memory usage (in MB) for any user session. The default value is 10 MB.

Description	How to Set It
Number of user sessions to display	Specify the number of user sessions with the highest memory utilization that you want displayed in the event detail message. Enter 0 if you want to see information for all user sessions. The default value is 15 user sessions.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).

TopResourceConsumingSQL

Use this Knowledge Script to determine which SQL queries for Oracle database are consuming the most resources on their UNIX hosts. This script identifies the top *N* queries consuming the most memory, disk I/O, and CPU time. The job raises an event with results of the job, and/or if the job results in a failure to retrieve data.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
DBA_USERS
V$SQLAREA
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and collects the *N* SQL queries using the most CPU time, disk I/O, and memory.

Default Schedule

The default schedule for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for top resource-consuming SQL statements?	Set to **y** to collect data for charts and reports. If data collection is enabled, returns the top *N* SQL statements consuming the most resources. The parameters below let you choose which resources to monitor. Set a value for *N* using the **Number of SQL statements to retrieve** parameter. By default, data is not collected.
Monitor SQL statements consuming the most disk I/O?	Select the **Yes** check box to monitor SQL statements consuming the most disk I/O. By default, disk I/O is monitored.
Monitor SQL statements consuming the most memory?	Select the **Yes** check box to monitor SQL statements consuming the most memory. By default, memory usage is monitored.
Monitor SQL statements consuming the most CPU time?	Select the **Yes** check box to monitor SQL statements consuming the most CPU time. By default, CPU utilization is monitored. **Note** You cannot use this metric on Oracle databases prior to version 9.0.
Number of SQL statements to retrieve	The number of most executed SQL queries to be retrieved by the job. The default value is 10. The maximum is 30.

Description	How to Set It
Raise event if error occurs during retrieval?	Select the **Yes** check box to raise an event when an error occurs during job execution. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 10 (red event indicator.
Raise event with results from query?	Select the **Yes** check box to raise an event with the results of the query. By default, the job does not raise events.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 40 (magenta event indicator).

Transaction

Use this Knowledge Script to monitor the following parameters:

- **Active Transactions**: retrieve the number of active transactions that are ongoing, and the maximum number of transactions that can be executed concurrently (set as an initialization parameter). This script computes a ratio, expressed as a percentage, of the two numbers. When you enable data collection, the percentage is stored in the repository. You can set multiple thresholds for the maximum ratio, and the job raises an event when any of the thresholds exceeds the value you specified.
- **Call Rate**: the demand placed on a database instance from all sources. This demand is determined by tracking the number of database calls per second from all applications and processes accessing the database `instance.` The database calls that are tracked include `Parse, Execute`, and `Fetch` statements. These calls are sometimes described as **user calls**. When the call rate (and thus the workload demand on the server) exceeds the threshold you set, the job raises an event.
- **Calls Per Transaction**: the demand placed on a database instance by each transaction. This demand is determined by tracking the number of database calls (for example, to parse, execute, and fetch data) per committed transaction. When the number of database requests per transaction exceeds the threshold, the job raises an event.
- **Transaction Rate**: the transaction rate for an Oracle database. This script tracks the number of transactions per second to provide a basic measurement of application workload. In addition, this script raises an event if the number of transactions per second exceeds the threshold you set.

  Changes to your applications or to application usage patterns can affect the transaction rate, but in general, an increase in the transaction rate suggests an increase in overall server load. If you see a decrease in the transaction rate with the same number of connected users, it may indicate that you need to do some database tuning or investigate the reasons for the changes.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION

V$PARAMETER
V$TRANSACTION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Monitoring	
Monitor ratio of active transactions?	Set to **y** to monitor the ratio of active transactions.
Monitor call rate?	Set to **y** to monitor the ratio of call rate.
Monitor calls made per transaction?	Set to **y** to monitor the calls made per transaction.
Monitor transaction rate?	Set to **y** to monitor the transaction rate.
Event Notification	
Event option for the ratio of active transactions to maximum concurrent transactions	
Raise event if ratio exceeds threshold?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job raises events.
Threshold - ratio of active transactions to max concurrent transactions	Specify a threshold for the maximum ratio of active transactions to maximum concurrent transactions, expressed as a percentage. The default for this threshold is 95%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 5 (red event indicator).
Raise event if ratio exceeds threshold?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold - ratio of active transactions to max concurrent transactions	Specify a threshold for the maximum ratio of active transactions to maximum concurrent transactions, expressed as a percentage. The default for this threshold is 80%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 15 (yellow event indicator).
Raise event if ratio exceeds threshold?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold - ratio of active transactions to max concurrent transactions	Specify a threshold for the maximum ratio of active transactions to maximum concurrent transactions, expressed as a percentage. The default for this threshold is 60%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 25 (blue event indicator).

Description	How to Set It
Raise event if ratio exceeds threshold?	Select the **Yes** check box to raise an event if the threshold exceeds the value you specified. By default, the job does not raise events.
Threshold - ratio of active transactions to max concurrent transactions	Specify a threshold for the maximum ratio of active transactions to maximum concurrent transactions, expressed as a percentage. The default value is 40%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 35 (magenta event indicator).
Event option for call rate	
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the maximum number of calls per second exceeds the threshold. By default, the job raises events.
Threshold -- Maximum call rate	Enter a threshold for the maximum number of calls per second allowed before the job raises an event. The default value is 100 calls per second.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).
Event option for calls made per transaction	
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the number of calls per transaction exceeds the threshold. By default, the job raises events.
Threshold -- Maximum number of calls per transaction	Enter a threshold for the maximum number of database calls per transaction allowed before the job raises an event. The default value is 100 calls per transaction.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).
Event option for transaction rate	
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the transaction rate exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum transaction rate	Enter a threshold for the maximum number of transactions per second allowed before an event is raised. The default value is 1 transaction per second.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).
Collect Data	
Collect data for the ratio of active transactions to maximum concurrent transactions?	Set to **y** to collect data for charts and reports. If you enable data collection, the Knowledge Script returns the ratio of active transactions to maximum concurrent transactions as a percentage (%). By default, data is not collected.

Description	How to Set It
Collect data for call rate?	Set to **y** to collect data for charts and reports. If you enable data collection, the Knowledge Script returns the total user calls per second for all work sources. By default, data is not collected.
Collect data for calls made per transaction?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the current transaction rate (transactions/second). By default, data is not collected.
Collect data for transaction rate?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the current transaction rate (transactions/second). By default, data is not collected.

TransactionRate

Use this Knowledge Script to monitor the transaction rate for an Oracle database. This script tracks the number of transactions per second to provide a basic measurement of application workload. In addition, this script raises an event if the number of transactions per second exceeds the threshold you set.

Changes to your applications or to application usage patterns can affect the transaction rate, but in general, an increase in the transaction rate suggests an increase in overall server load. If you see a decrease in the transaction rate with the same number of connected users, it may indicate that you need to do some database tuning or investigate the reasons for the changes.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for transaction rate?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the current transaction rate (transactions/second). By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the transaction rate exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum transaction rate	Enter a threshold for the maximum number of transactions per second allowed before an event is raised. The default value is 1 transaction per second.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10 (red event indicator).

UpdateInstances

Use this Knowledge Script to update the list of Oracle databases/instances on each UNIX host.

Note This script cannot be run to update environments in all cases. If you do not use a `listener.ora` file to maintain listener information, or if you install a new Oracle version on the host, we recommend that you log in to the host and run the `ckoracle` utility. This utility will prompt you to enter required information for newly added or deleted Oracle databases/instances.

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Notes

You must run the Discovery_OracleUNIX script after running the UpdateInstances script to pick up any changes in the environment.

If databases have been deleted, you must delete the Oracle UNIX objects from the TreeView. This cannot be done by the module or AppManager itself.

Default Schedule

The default interval for this script is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Required Parameter(s)	
Oracle Home to use as the client (usually that of the newest Oracle version)	Specify the Oracle Home directory that should be used as the client. If multiple versions of Oracle RBDMS are installed on the host, this is usually the Oracle Home directory of the newest version of Oracle. The default value is blank.
Optional Parameter(s)	
Location of `sqlnet.ora`, `listener.ora`, `tnsnames.ora (TNS_ADMIN)`	Specify the directory where the Oracle Net/Net 8 files reside (such as the `tnsnames.ora`, `listener.ora`, and `sqlnet.ora`). It is only necessary to set this parameter when the files are not in the default location for each Oracle Home (`$ORACLE_HOME/network/admin`). The default value is blank.
Oracle Username	Enter the username that OracleUNIX jobs will use for authentication with Oracle RDBMS during execution. This username will be passed to the NetIQ Security Manager. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.

Description	How to Set It
Password for the Oracle Username	Specify the password for the Oracle Username specified in the previous parameter. This password will be encrypted and passed to the AppManager Security Manager along with the Oracle username. The default value is blank.
Are all databases using the same listener?	Select the **Yes** check box if one listener is being used on the UNIX host, then specify the details of that listener below. By default, this parameter is disabled.
Name of listener	Specify the name of the listener that is being used on the UNIX host. This parameter is only used when you set the **Are all databases using the same listener?** to **Yes**. The default value is `LISTENER`.
Port used by listener	Enter the port number of that the listener is listening on for the UNIX host. This parameter is only used when you set the **Are all databases using the same listener?** to **Yes**. The default value is 1521.
Raise event if error occurs updating instances?	Select the **Yes** check box to raise an event when an error is detected while attempting to update the list of Oracle instances. By default, events are enabled.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 10 (red event indicator).
Raise event with current instance info if successfully updated?	Select the **Yes** check box to raise an event with the information collected on Oracle instances on the host during the update. By default, the job does not raise events.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event for successfully setting the monitoring options. The default severity level is 40 (magenta event indicator).

User

Use this Knowledge Script to monitor the following parameters:

- **User Calls Per Parse**: the ratio of parse count (hard) to the number of user calls as a percentage. The number of user calls that result in a parse indicates how well an application is managing its context area. Changes in this ratio may indicate changes to the application itself, or to changing usage patterns (For example, because users are moving from one module to another, more or less frequently).

  Generally, if the ratio of parsed calls to total user calls is low, it indicates that the SQL statements are executing efficiently without frequent reparsing. Otherwise, it may indicate that the private SQL area is too small.

  This script raises an event when the percentage of user calls that are parsed exceeds the threshold you set.

- **User Sessions**: the total number of user sessions accessing an Oracle database. If the total number of user sessions crosses the threshold, the job raises an event.

  You can specify the number of user sessions to display in the Event Properties dialog box. The Event Properties dialog box displays the total number of user sessions exceeding the threshold. Information in the graph includes the number of sessions for each user and the username.

- **User Rollback Ratio**: the user rollback ratio for an Oracle Database. The user rollback ratio indicates the percentage of attempted application transactions that fail. The ratio compares the number of transactions rolled back to the total number of transactions attempted.

  Because rolling back a transaction uses significant system resources, an increase in this ratio suggests resources have been wasted in attempting to execute failed transactions. If you see a continued increase in this ratio, it may indicate serious application or database performance problems. This script raises an event when the rollback ratio exceeds the threshold.

- **Blocking Sessions**: the user sessions that are blocking other sessions and processes from accessing the Oracle database. You can set a maximum threshold for the number of sessions that are allowed to block other sessions and processes. If the number of blocking sessions exceeds the threshold, the job raises an event.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$LOCK
V$VERSION

DBA_USERS
V$SESSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
User	
User Calls Per Parse	Select the **Yes** check box to monitor User Calls Per Parse.
User Sessions	Select the **Yes** check box to monitor User Sessions.
User Rollback Ratio	Select the **Yes** check box to monitor User Callback Ratio.
Blocking Sessions	Select the **Yes** check box to monitor Blocking Sessions.
Event Notification	
Raise event if threshold is exceeded for User Calls Per Parse?	Select the **Yes** check box to raise an event if the ratio of parses per user call exceeds the threshold you set. By default, the job raises events.
Raise event if threshold is exceeded for User Sessions?	Select the **Yes** check box to raise an event if the number of user sessions exceeds the threshold. By default, the job raises events.
Raise event if threshold is exceeded for User Rollback Ratio?	Select the **Yes** check box to raise an event if the number of user transaction rollbacks exceeds the threshold. By default, the job raises events.
Raise event if threshold is exceeded for Blocking Sessions?	Select the **Yes** check box to raise an event if the number of blocking sessions exceeds the threshold you set. By default, the job raises events.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).
Data Collection	
Collect data for User Calls Per Parse?	Select the **Yes** check box to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the current percentage of user calls that are parsed. By default, data is not collected.
Collect data forUser Sessions?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the total number of user sessions. By default, data is not collected.
Collect data for User Rollback Ratio?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the current user rollback ratio. By default, data is not collected.
Collect data for Blocking Sessions?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the number of blocking sessions per interval. By default, data is not collected.
Monitoring	

Description	How to Set It
Threshold -- Maximum Parses Per User Call	Enter a threshold for the maximum ratio of parsed calls to total user calls allowed before an event is raised. The default value is 0.2.
Threshold -- Maximum total user sessions	Enter a threshold for maximum number of user sessions. The default value is 75 user sessions.
Number of user sessions to display	Specify the number of user sessions you want displayed in the Event Properties dialog box. Enter 0 if you want all user sessions displayed. The default value is 10 user sessions.
Threshold -- Maximum user rollback ratio	Enter a threshold for the maximum percentage of transaction rollbacks allowed before the job raises an event. The default value is 75%.
Threshold -- Maximum number of blocking sessions	Enter a threshold for the maximum number of user sessions allowed to block other user sessions and processes during the monitoring interval. The default value is 10 sessions.

UserCallsPerParse

Use this Knowledge Script to monitor the ratio of parse count (hard) to the number of user calls as a percentage. The number of user calls that result in a parse indicates how well an application is managing its context area. Changes in this ratio may indicate changes to the application itself, or to changing usage patterns (For example, because users are moving from one module to another, more or less frequently).

Generally, if the ratio of parsed calls to total user calls is low, it indicates that the SQL statements are executing efficiently without frequent reparsing. Otherwise, it may indicate that the private SQL area is too small.

This script raises an event when the percentage of user calls that are parsed exceeds the threshold you set.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for parses per user call?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the current percentage of user calls that are parsed. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the ratio of parses per user call exceeds the threshold you set. By default, the job raises events.
Threshold -- Maximum ratio of parses per user call	Enter a threshold for the maximum ratio of parsed calls to total user calls allowed before an event is raised. The default value is 0.2.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

UserRollbackRatio

Use this Knowledge Script to monitor the user rollback ratio for an Oracle Database. The user rollback ratio indicates the percentage of attempted application transactions that fail. The ratio compares the number of transactions rolled back to the total number of transactions attempted.

Because rolling back a transaction uses significant system resources, an increase in this ratio suggests resources have been wasted in attempting to execute failed transactions. If you see a continued increase in this ratio, it may indicate serious application or database performance problems. This script raises an event when the rollback ratio exceeds the threshold.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
V$SYSSTAT
V$VERSION
```

Resource Objects

Oracle Database folders. When you drop a script on an Oracle Database folder, a job executes on that database and monitors only that database.

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for user rollback ratio?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the current user rollback ratio. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the number of user transaction rollbacks exceeds the threshold. By default, the job raises events.
Threshold -- Maximum user rollback ratio	Enter a threshold for the maximum percentage of transaction rollbacks allowed before the job raises an event. The default value is 75%.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

UserSessions

Use this Knowledge Script to monitor the total number of user sessions accessing an Oracle database. If the total number of user sessions crosses the threshold, the job raises an event.

You can specify the number of user sessions to display in the Event Properties dialog box. The Event Properties dialog box displays the total number of user sessions exceeding the threshold. Information in the graph includes the number of sessions for each user and the username.

The account you use to run this script must have `SELECT` permissions for the following tables:

```
DBA_USERS
V$SESSION
```

Resource Objects

Oracle Server icon, or Oracle icon. When dropped on the Oracle Server icon, a single script job monitors every database on that server. When dropped on an Oracle icon, the script monitors only that database.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Oracle Username	Enter the username that this script needs to access the target databases. If you run this script on more than one database, configure each database with the same username. **Note** To use SYSDBA authentication, leave this parameter blank. The default value is blank.
Collect data for number of user sessions?	Set to **y** to collect data for charts and reports. When you enable data collection, the Knowledge Script returns the total number of user sessions. By default, data is not collected.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the number of user sessions exceeds the threshold. By default, the job raises events.
Threshold -- Maximum total user sessions	Enter a threshold for maximum number of user sessions. The default value is 75 user sessions.
Number of user sessions to display	Specify the number of user sessions you want displayed in the Event Properties dialog box. Enter 0 if you want all user sessions displayed. The default value is 10 user sessions.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

Chapter 59
PhoneQuality Knowledge Scripts

The PhoneQuality category provides the following Knowledge Scripts for monitoring the voice quality of Cisco IP phones.

From the Knowledge Script view of Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AddCiscoPhone	Adds a Cisco IP phone to the TreeView pane.
CiscoPhoneQuality	Polls Cisco phones for voice quality statistics.
RemovePhone	Removes an IP phone from the TreeView pane.

AddCiscoPhone

Use this Knowledge Script to add a Cisco IP phone to the TreeView pane. You must add a phone before you can monitor it with the CiscoPhoneQuality script.

When polling a phone to get device information, the managed object has a 20-second timeout period for each phone that it is attempting to contact. If you are adding many phones at one time, this Knowledge Script job may take quite a while if phones cannot be contacted.

Note
If you use the Cisco CallManager Extension Mobility feature, then you know that it allows a Cisco IP phone to assume different configurations based on the user who is logged into the phone. When you add an Extension Mobility-enabled phone with the AddCiscoPhone script, the details of the phone, including directory number, are also based on the user who is logged in. If no user is logged in, then phone details are based on your CallManager configuration. In some cases, the phone details may indicate a directory number of 0000. In others, the phone may not be added at all because the CallManager configuration for the directory number is blank. NetIQ Corporation recommends that you add the phone at a time when the regular user is logged on.

Resource Object

PHONEQ_CISCOPHONEF

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the AddCiscoPhone job fails. The default is 5.
Configuration Settings	
List of Cisco phone IP addresses	Type the IP addresses in dotted notation, of the Cisco phone that you want to monitor. You can type one address or a list of addresses. If you type a list, separate the addresses with a comma, like so: `10.46.4.15,10.46.4.149`. **Note** If you have more addresses than is convenient to enter in this field, you can list the addresses in a separate file and then use the following parameter to access that file.

Description	How To Set It

Full path to file with list of Cisco phone IP addresses	Type the full path to a file that contains a list of the IP addresses. Each address in the file should be on a separate line, like so:
	`10.46.4.15`
	`10.46.4.149`
	Because the file must be accessible from the agent, the path must be a local directory on the agent computer or a UNC path.
	Important If you type a UNC path, then the `netiqmc` service must be running as a user that has access to the path.

Event Notification	
Raise event if phone added successfully?	Set to **Yes** to raise an event if the phone is successfully added to the TreeView pane. The default is Yes.
Event severity when phone added successfully	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the phone is added successfully. The default is 25.
Raise event if phone cannot be added?	Set to **Yes** to raise an event if the phone cannot be added to the TreeView pane. The default is Yes.
Event severity when phone cannot be added	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the phone cannot be added to the TreeView pane. The default is 40.

CiscoPhoneQuality

Use this Knowledge Script to poll Cisco IP phones for voice quality statistics on active calls. Among the details within a quality data stream is the following information:

- Remote IP address and port number
- Number of datagrams sent and lost for packet loss statistics
- Codec for MOS and R-value statistics

Although this information can be very useful, over time it can take up a significant amount of space in the repository. If you want, you can gather only data points, and not the information discussed above. Simply click on the **Advanced** tab and select **Collect only data point** in the Data options panel.

Configuring a Diagnosis Action

If you use NetIQ Vivinet Diagnostics to diagnose call quality problems between your IP phones, you can use the **Actions** tab to configure Action_DiagnoseVoIPQuality to trigger Vivinet Diagnostics run a diagnosis when an event is raised.

Click the **Actions** tab, and then click **New**. In the **Action** list, select **Action_DiagnoseVoIPQuality**. Click **Properties** and set the parameters for the Action script. For more information, see the script's Help.

Resource Object

PHONEQ_CISCOPHONEOBJ

Default Schedule

The default schedule is **Asynchronous**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the failure of the CiscoPhoneQuality job. The default is 5.
Monitor Settings	
Polling interval when no call is in progress	Specify the number of seconds that will elapse between polling instances when no call is in progress. The default is 120 seconds.
Polling interval when call is in progress	Specify the number of seconds that will elapse between polling instances when a call *is* in progress. The default is 30 seconds.

Description	How To Set It
Additional fixed delay for MOS/R-value calculation	Enter an amount of delay (in milliseconds) that you want to add to a call. This amount of delay is in addition to the three other types of delay that are associated with calculating MOS and R-value: • Network delay in one direction. This value is not available from the phones and so is set to 0 for calculating MOS and R-value. A network delay of 0 provides a “Listening” MOS/R-value because it does not take into consideration the interaction of a t wo-way conversation. • Packetization delay. This value is fixed, based on the type of codec being used. • Jitter buffer delay. This value is fixed, based on the type and size of the jitter buffer being used.
Event Notification	
Raise event if error occurs during polling?	Set to **Yes** to raise an event if an error occurs during the polling of the selected IP phone. The default is Yes. Among the possible errors are the inability of AppManager to contact the IP phone and the improper formatting of the gathered statistics.
Event severity when error occurs during polling	Set the event severity level, from 1 to 40, to reflect the importance of an event in which an error occurred during phone polling. The default is 5.
Monitor Listening MOS	
Event Notification	
Raise event if Listening MOS falls below threshold?	Set to **Yes** to raise an event if the value of Listening MOS falls below the threshold that you set. The default is Yes.
Threshold - Minimum Listening MOS	Specify the lowest Listening MOS value that can be calculated before an event is raised. The default is 3.6.
Event severity when Listening MOS falls below threshold	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the Listening MOS value falls below the threshold you set. The default is 5.
Data Collection	
Collect data for Listening MOS?	Set to **Yes** to collect Listening MOS data for charts and graphs. The default is Yes.
Monitor Listening R-value	
Event Notification	
Raise event if Listening R-value falls below threshold?	Set to **Yes** to raise an event if the Listening R-value falls below the threshold that you set. The default is unchecked.
Threshold - Minimum Listening R-value	Enter the lowest Listening R-value that can be calculated before an event is raised. The default is 70.
Event severity when Listening R-value falls below threshold	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the Listening R-value falls below the threshold you set. The default is 5.
Data Collection	
Collect data for Listening R-value?	Set to **Yes** to collect Listening R-value data for charts and graphs. The default is unchecked.
Monitor Average Jitter	
Event Notification	
Raise event if average jitter exceeds threshold?	Set to **Yes** to raise an event if the amount of average jitter exceeds the threshold that you set. The default is Yes.

Description	How To Set It
Threshold - Maximum average jitter	Specify the highest amount of average jitter that can be achieved before an event is raised. The default is 60 milliseconds.
Event severity when average jitter exceeds threshold	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the amount of average jitter exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for average jitter?	Set to **Yes** to collect average jitter data for charts and graphs. The default is Yes.
Monitor Maximum Jitter	
Event Notification	
Raise event if maximum jitter exceeds threshold?	Set to **Yes** to raise an event if the amount of maximum jitter exceeds the threshold that you set. The default is Yes.
Threshold - Highest maximum jitter	Specify the highest amount of maximum jitter that can be achieved before an event is raised. The default is 60 milliseconds.
Event severity when maximum jitter exceeds threshold	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the amount of maximum jitter exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for maximum jitter?	Set to **Yes** to collect maximum jitter data for charts and graphs. The default is Yes.
Monitor Interval Packet Loss	
Event Notification	
Raise event if interval packet loss exceeds threshold?	Set to **Yes** to raise an event if the percentage of interval packet loss exceeds the threshold that you set. The default is Yes.
Threshold - Maximum interval packet loss	Specify the highest percentage of interval packet loss that can occur before an event is raised. The default is 1%.
Event severity when interval packet loss exceeds threshold	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the percentage of interval packet loss exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for interval packet loss?	Set to **Yes** to collect interval packet loss data for charts and graphs. The default is Yes.

RemovePhone

Use this Knowledge Script to remove an IP phone from the TreeView pane.

When this Knowledge Script job runs successfully, the data source object in the TreeView pane is deleted. In addition, the job itself is also deleted, which is a normal side-effect of removing a TreeView object. The event that this job creates is not deleted because it is associated with the parent object (`PhoneQuality:<computer name>` object). However, if you set the global preference to "Remove associated events when jobs are deleted," then even the event is deleted when the object and job are deleted. To set global preferences, select **File > Preferences > Repository > Event** in the AppManager Operator Console.

Tips

- After dropping this script on the object of the phone that you want to remove, double-check your selection in the **Objects** tab. By specifically selecting a phone object from the **Objects** tab, you will not accidentally remove a phone that you want to keep.
- Before attempting to remove a phone, stop any monitoring jobs that are running on the phone.

Resource Object

PHONEQ_CISCOPHONEOBJ

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the failure of the RemovePhone job. The default is 5.
Event Notification	
Raise event if phone removal succeeds?	Set to **Yes** to raise an event if the phone is successfully removed from the TreeView pane. The default is Yes.
Event severity when phone removal succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the phone is successfully removed from the TreeView pane. The default is 25.
Raise event if phone removal fails?	Set to **Yes** to raise an event if the phone removal attempt fails. The default is Yes.
Event severity when phone removal fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the phone removal attempt fails. The default is 15.

Chapter 60
PowerShell Knowledge Scripts

AppManager for Microsoft Windows provides the following Knowledge Scripts for monitoring the PowerShell scripting and command environment. PowerShell is made up of hundreds of executable objects called *cmdlets*, pronounced command-lets.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
RunCommand	Runs a specified PowerShell command.

RunCommand

Use this Knowledge Script to run the Microsoft Windows PowerShell `cmdlet` or PowerShell script (`.PS1` file) you specify. This script raises an event with the command results and generates a datastream with the value returned by the command.

You can also use this script to run any command that can be run from a Windows command prompt, such as `dir c:\temp`. PowerShell accepts commands in `cmdlet`, `.PS1`, and Windows `cmd.exe` formats.

Prerequisites

- Microsoft Windows PowerShell version 1.0
- Microsoft .NET Framework version 3.0
- AppManager for Windows version 7.6, at minimum

Resource Object

PowerShell folder

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Event Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the RunCommand job fails. The default is 5.
PowerShell Command	

Parameter	How to Set It

PowerShell command to run	Provide the PowerShell `cmdlet`, PowerShell script, or Windows command you want to run. You can string multiple commands together. For example:
	`dir c:\temp | findstr /I log`
	Ensure your command contains no syntax errors. The RunCommand job will fail if the command contains syntax errors.
	Hint Double quotation marks within a command must be paired with another set of quotation marks. In other words, if your command contains a string that is contained within a set of quotation marks, enter the string so that it is contained within two sets of quotation marks. For example:
	`""my command""`
	The double quotation marks are replaced with a backward apostrophe (a *backtick*, which is accepted by Powershell) before the command is run.
	Restrictions
	• File pathnames in PowerShell scripts cannot contain spaces. Pathnames such as `c:\Program Files\...` cause the RunCommand job to fail.
	• PowerShell scripts (`.PS1` files) must be located on the computer on which you run the RunCommand script. The RunCommand script cannot run remote PowerShell scripts.

Event Notification	
Raise event with result of command?	Select **Yes** to raise an event when the command you run returns text or numeric results. The default is Yes.
Format results as	Select whether to format command results in a **Table** or a **List** or to apply no formatting. The default is Table. Select **Unformatted** if the command returns results that are already formatted.
Event title	Provide text to use as the title of the event.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a command returns text or numeric results. The default is 25.
Raise event only if result contains specified pattern?	Select **Yes** to raise an event if the command returns text that matches the expression you provide in the *Expression to match against results* parameter. The default is unselected. This parameter is valid only if the *Raise event with result of command* parameter is enabled.
Pattern to find in the results	Provide the text you want to compare to the command results. The following wildcards are acceptable: • ***** - matches zero or more instances of a character. • **?** - matches exactly one instance of a character. • **[]** - matches exactly one instance of any character between the square brackets, including ranges. Examples: • `[abc][def]` matches “ad,” “bad,” and “ace,” but not “bleary.” • `[a-z][a-z]` matches text that contains two adjacent alphabetic characters. • `foo? Bar` matches “food bar” and “This is a food bar!” but not “foobar” or “foo bar.” • `*maximum mailbox*` matches “user smith has reached maximum mailbox size.”

Parameter	How to Set It
Raise event only if numeric result crosses threshold?	Select **Yes** to raise an event if the command returns a numeric value that exceeds or falls below the threshold you set in the *Threshold value parameter*. The default is unselected. This parameter is valid only if the *Raise event with result of command* parameter is enabled.
Select operator to compare numeric result to threshold	Select the operator with which to compare the command results to the threshold value. Choose from one of the following: • Greater than • Less than • Greater than or equal to • Less than or equal to An event is raised if the command results do not match the threshold value based on the operator you choose. The default is Greater than.
Threshold value	Provide the numeric value to compare with the command results. An event is raised if the command results do not match the threshold value based on the option you choose in the *Select operator to compare numeric result to threshold* parameter. The default is 0.
Metric name to include in event title	Provide the name of the metric for which the command returns numeric results. For example, specify the name of a Performance Monitor counter. The name of the metric will be part of the title of the event raised when the numeric result crosses the threshold.
Raise event if command returns no results?	Select **Yes** if the command you run returns no results. The default is unselected. **Hint** You can use this parameter to raise an event when a command that *should* return text or numeric results does not return any results. Enable this parameter and disable the *Raise event with result of command?* parameter.
Event severity when command returns no results	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a command does not return text or numeric results. The default is 5.
Data Collection	
Collect data for numeric command result?	Select **Yes** to collect data for charts and reports. This parameter is valid only if the *Raise event only if numeric result crosses threshold?* parameter is enabled. The default is unselected. Use the following parameters to format the wording and units of datastream legends.
Name of monitored metric	Provide the name of the metric for which the command returns numeric results. For example, specify the name of a Performance Monitor counter. The name of the metric will be part of the datastream legend.
Name of monitored resource	Provide the name of the device associated with the metric for which the command returns numeric results. For example, specify the hostname of a computer. The name of the device will be part of the datastream legend.
Datastream units	Identify the unit of measure associated with the metric for which the command returns numeric results. For example, specify `MB` or `Mbytes`. The unit of measure will be part of the datastream legend.

Chapter 61
ReportAM Knowledge Scripts

The ReportAM category provides the following Knowledge Scripts for generating reports based on data collected by Knowledge Script jobs.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	Description
AgentMaintenance	The maintenance history of any computer on which you installed an AppManager agent.
AggValueHistory	Average, minimum, or maximum values aggregated by hour, day, week, or month over a specified time period.
ApplicationInfo	The monitored applications on computers in your AppManager environment.
AvgMaxMinValue	The average, maximum and minimum values of data streams collected by Knowledge Script jobs.
AvgValueByDay	The average daily value of data streams collected by Knowledge Script jobs.
AvgValueByHr	The average values per hour of data streams collected by Knowledge Script jobs.
AvgValueByMin	The average values per minute of data streams collected by Knowledge Script jobs.
Chart2HTML	Converts the contents of an XML file to an HTML page containing a chart and/or table of AppManager repository data.
Compare24Hours	Twenty-four average, minimum, or maximum hourly values for today, last week, last month, and the last three months.
Compare24HoursLD	Twenty-four average, minimum, or maximum hourly values for today, last week, last month, and the last three months. Use this report for data sets over 1.5 GB.
CompDeploy	The total number of instances of each AppManager component installed on computers in an AppManager site.
CompLic	Summary of AppManager license compliance.
CompVersion	The version number of AppManager components installed on all computers in an AppManager site.
CurrentDiskSpaceUsage	The used and free space on logical disks.
DataStream	High-level information about data streams collected by Knowledge Script jobs.

Knowledge Script	Description
DataSummary	Statistical analysis of selected data streams.
DeletedObjects	Objects that have been permanently deleted from the Operator Console TreeView.
DetailData	Information returned by Knowledge Scripts that prepare data for presentation in an XML format.
DFSSummary	Details of the Distributed File System service on specified computers.
EventArchiveSummary	Summary of events from the ArchiveEvent table in the AppManager repository.
EventSeveritySummary	Number and severity of events raised by Knowledge Script jobs on specified computers.
EventStatisticsSummary	Summary of events per computer, listed by monitored application.
EventSummary	Summary of events per computer.
FRSSummary	Details of the File Replication service on specified computers.
GeneralCounter	Average, maximum or minimum value of selected data streams.
GeneralMachineDown	Computers that were detected as down during a specified time period.
GroupPolicySummary	Summary of Group Policy settings for specified computers.
Inventory	Details of a specified application on a computer, or all components of a computer.
JobInfo	Details of Knowledge Script jobs.
JobSummary	Knowledge Script job, monitoring policy, action, and event information for each computer in an AppManager repository.
LastDataPoint	Value of the most recently collected data point in a data stream.
ModuleUsage	The number of different AppManager modules in use.
NetworkInterface	Details of the network interface components on specified computers.
NTLogicalDisk	Details of the logical disks on specified computers.
NTPhysicalDisk	Details of the physical disks on specified computers.
PerfOverview	A separate chart for each selected data stream.
PerfOverviewLD	A separate chart for each selected data stream. Use this report for data sets over 1.5 GB.
PlainDataInfo	Details of data points in specified data streams.
PrinterSummary	Details of the printers and printer drivers installed on specified computers.
SerLevAvailability	Percentage of time specified services were up or down.
SQLDBInfo	Details of the databases managed by SQL Servers on specified computers.
SystemUpTime	Up- and downtime (by percent) of monitored computers.
SystemUpTimePie	Up- and downtime (by percent) of monitored computers. This report uses only a pie chart.
WatchList	Top or bottom N computers (by number or percent) generating the selected data streams.

AgentMaintenance

Use this Knowledge Script to generate a report about the maintenance history of any computer on which you installed an AppManager agent. The report lists the type of maintenance (scheduled or ad hoc), and the beginning and ending dates and times of the maintenance period.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer name.
Select time range	Filter data in your report by a specific or sliding time range. The default is Sliding
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

AggValueHistory

Use this Knowledge Script to generate a report from data in the archive and aggregate tables.

If you choose to move data from the archive table to the aggregate tables, that data is then aggregated by hour, day, and month.

Briefly, the aggregation process works as follows:

- A preference is specified for the number of months' worth of data to keep in the archive table (for example, the three most recent months' worth).

  For all older data, an hourly average, minimum, maximum, sum, and count value are calculated. Those hourly values are then moved to the hourly aggregate table: ArcAvgHourlyData. Each hour's worth of data is then represented by five data points: average, minimum, maximum, sum, and count.

- The hourly aggregate table keeps three months' worth of data.

  For all older data, a daily average, minimum, maximum, sum, and count value are calculated. Those daily values are then moved to the daily aggregate table (ArcAvgDailyData). Each day's worth of data is then represented by five data points (average, minimum, maximum, sum, and count).

- The daily aggregate table keeps six months' worth of data.

  For all older data, a monthly average, minimum, maximum, sum, and count value are calculated. Those monthly values are then moved to the monthly aggregate table (ArcAvgMonthlyData). Each month's worth of data is then represented by five data points (average, minimum, maximum, sum, and count).

- The monthly aggregate table keeps data indefinitely.

Once information is moved from the source table to the destination table, it is deleted from the source table.

This script lets you generate a report that gives the hourly, daily, weekly, or monthly average, minimum or maximum value for selected data streams over the time range you specify (for example, the monthly average of memory used by SQL Server processes over the last year).

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.

Parameter	How To Set It
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **By Knowledge Script** provides links to pages showing all data streams collected by a Knowledge Script (each page shows all data streams collected from all computers on which the script has run) • **All data streams on one page** generates a report with all data on a single page
Select time range	Filter the data in your report by a specific or sliding time range. The default is Sliding.
Select average, minimum, or maximum	Select the type of value you want to represent in your report.
Aggregation interval	Select the time period by which the data in your report is aggregated: • Hourly • Daily • Weekly • Monthly
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.

Parameter	How To Set It
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

ApplicationInfo

Use this Knowledge Script to generate a report detailing the monitored applications on computers in your AppManager environment. Details include application and build numbers, installation directories, and path and log information.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computers	Filter the data in your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

AvgMaxMinValue

Use this Knowledge Script to generate a report detailing the average, maximum and minimum values of data streams collected by Knowledge Script jobs.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Select peak weekday(s)	Filter the data for your report by the days of the week.
Aggregation interval	Select the number of hours by which the data in your report is aggregated.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.
Series style (average)	Select a graphical style for the average value series in the charts in your report.
Chart title	Provide a title for the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.

Parameter	How To Set It
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

AvgValueByDay

Use this Knowledge Script to generate a report detailing the average daily value of data streams collected by Knowledge Script jobs.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **By Knowledge Script** provides links to pages showing all data streams collected by a Knowledge Script (each page shows all data streams collected from all computers on which the script has run) • **All data streams on one page** generates a report with all data on a single page
Select time range	Filter the data for your report by a specific or sliding time range.
Select peak weekday(s)	Filter the data for your report by the days of the week.
Aggregation interval	Select the number of days by which the data in your report is aggregated.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.

Parameter	How To Set It
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

AvgValueByHr

Use this Knowledge Script to generate a report detailing the average values per hour of data streams collected by Knowledge Script jobs.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **By Knowledge Script** provides links to pages showing all data streams collected by a Knowledge Script (each page shows all data streams collected from all computers on which the script has run) • **All data streams on one page** generates a report with all data on a single page
Select time range	Filter the data in your report by a specific or sliding time range. The default is Sliding.
Select peak weekday(s)	Filter the data in your report by days of the week.
Aggregation interval	Select the number of hours by which the data in your report is aggregated.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.

Parameter	How To Set It
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

AvgValueByMin

Use this Knowledge Script to generate a report detailing the average values per minute of data streams collected by Knowledge Script jobs.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **By Knowledge Script** provides links to pages showing all data streams collected by a Knowledge Script (each page shows all data streams collected from all computers on which the script has run) • **All data streams on one page** generates a report with all data on a single page
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Select peak weekday(s)	Filter the data for your report by days of the week.
Aggregation interval	Select the number of minutes by which the data in your report is aggregated.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.

Parameter	How To Set It
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Chart2HTML

Use this Knowledge Script to generate an HTML page containing a chart and/or table of the data referenced in an XML file. Export data from a report to an XML file using the **Report to XML** command on the Export menu in the AppManager Chart Console.

To use this script successfully, the XML file must be saved to a folder accessible by the report agent.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
XML input file	Specify the full path to the .XML file generated from the AppManager Chart Console.
Select output folder	Set parameters for the output folder.
Chart type	Select the type of data display you want in the report: • Chart (chart only) • Data (table only) • Chart and Data (chart and table)
Time frame	Select the time frame for data in the report: • All (all data referenced by the XML file) • Today (any data from the day the report script is run -- 12 A.M. to 11:59:59 P.M.) • Yesterday (any data from the day before the report script is run -- 12 A.M. to 11:59:59 P.M.) • This Week (any data from the week during which the report script is run -- 12 A.M. Sunday to the time of the report) • This Month (any data from the month during which the report script is run -- 12 A.M. of the first day to the time of the report) • This Year (any data from the year during which the report script is run -- 12 A.M. January 1 to the time of the report)
Fit into one graph?	Set to **y** to fit all data into a single graph. The default is y.
Report title	Provide a title for the report.
Severity for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Compare24Hours

Use this Knowledge Script to generate a report that compares the average, minimum or maximum values per hour of selected data streams for periods of 1 day, 1 week, 1 month, and 3 months. You can limit the scope of the report by selecting data from specific days of the week (for example Monday through Friday only).

If you expect the data sets from which you are deriving values to exceed 1.5 GB, use the Compare24HoursLD Knowledge Script.

The time periods illustrated in the report are:

- Today
- Last Week
- Last Month
- Last 3 Months

For example:

- Today = 4-1-06, 12 A.M. to 11:59:59 P.M.
- Last Week = 3-24-06, 12 A.M. to 3-30-06, 11:59:59 P.M. (the previous seven days)
- Last Month = 3-1-06, 12 A.M. to 3-31-06, 11:59:59 P.M. (all days of the previous month; for example, if Today is any day in April, then Last Month = all days in March)
- Last 3 Months = 1-1-06, 12 A.M. to 3-31-06, 11:59:59 P.M. (all days of the previous three months; for example, if Today is any day in April, then Last 3 Months = all days in January, February, and March)

Twenty-four values are given for each time period, from 12 A.M. to 11 P.M. For each time period, the values are based on different quantities of data. For example:

- 12 A.M. Today is an average of one hour's worth of data (12 A.M. to 12:59:59 A.M. for one day)
- 12 A.M. Last Week is an average of seven hours' worth of data (12 A.M. to 12:59:59 A.M. for each day of the week)
- 12 A.M. Last Month is an average of 31 hours' worth of data (12 A.M. to 12:59:59 A.M. for each day of the month)
- 12 A.M. Last 3 Months is an average of 90 hours' worth of data (12 A.M. to 12:59:59 A.M. for each day of the three months)

This report always compares these four time periods, and so there is no option to select the time range.

All time periods are relative to the day you start the report.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select peak weekday(s)	Filter the data for your report by days of the week.
Select average, minimum, or maximum	Select the type of value you want to represent in your report.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style (Today)	Define the graphic properties of the chart in your report, and for the chart series representing values for the Today time period.
Series style (Last Time Periods)	Select the series style for the last three time periods represented in the report. This parameter lets you select a series style different from the Today series in order to easily differentiate the time periods.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Compare24HoursLD

Use this Knowledge Script instead of Compare24Hours when the data sets from which you are deriving values exceed the ADO limit of 1.5 GB. When data sets exceed this size limit, the report agent cannot process the data. Use this script to process data on the SQL Server managing the AppManager repository and return the aggregated value to the report agent.

Use this script to generate a report that compares the average, minimum or maximum values per hour of selected data streams for periods of 1 day, 1 week, 1 month, and 3 months. You can limit the scope of the report by selecting data from specific days of the week (for example Monday through Friday only).

The time periods illustrated in the report are:

- Today
- Last Week
- Last Month
- Last 3 Months

For example:

- Today = 4-1-06, 12 A.M. to 11:59:59 P.M.
- Last Week = 3-24-06, 12 A.M. to 3-30-06, 11:59:59 P.M. (the previous seven days)
- Last Month = 3-1-06, 12 A.M. to 3-31-06, 11:59:59 P.M. (all days of the previous month; for example, if Today is any day in April, then Last Month = all days in March)
- Last 3 Months = 1-1-06, 12 A.M. to 3-31-06, 11:59:59 P.M. (all days of the previous three months; for example, if Today is any day in April, then Last 3 Months = all days in January, February, and March)

Twenty-four values are given for each time period, from 12 A.M. to 11 P.M. For each time period, the values are based on different quantities of data. For example:

- 12 A.M. Today is an average of one hour's worth of data (12 A.M. to 12:59:59 A.M. for one day)
- 12 A.M. Last Week is an average of seven hours' worth of data (12 A.M. to 12:59:59 A.M. for each day of the week)
- 12 A.M. Last Month is an average of 31 hours' worth of data (12 A.M. to 12:59:59 A.M. for each day of the month)
- 12 A.M. Last 3 Months is an average of 90 hours' worth of data (12 A.M. to 12:59:59 A.M. for each day of the three months)

This report always compares these four time periods, and so there is no option to select the time range.

All time periods are relative to the day you start the report.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select peak weekday(s)	Filter the data for your report by days of the week.
Select average, minimum, or maximum	Select the type of value you want to represent in your report.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style (Today)	Define the graphic properties of the chart in your report, and for the chart series representing values for the Today time period.
Series style (Last Time Periods)	Select the series style for the last three time periods represented in the report. This parameter lets you select a series style different from the Today series in order to easily differentiate the time periods.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

CompDeploy

Use this Knowledge Script to generate a report detailing the total number of instances of each AppManager component installed on computers in an AppManager site (for example, the number of IIS and Exchange managed objects).

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

CompLic

Use this Knowledge Script to generate a report summarizing AppManager license compliance.

A separate license is required for each managed application on each computer. For example, if you are using AppManager to manage Microsoft SQL Server on ten different computers, then you are required to have ten licenses for AppManager for Microsoft SQL Server. If you are managing multiple instances of an application running on a single computer, such as multiple instances of SQL Server, only one license is required for that computer.

This report lists the number of AppManager licenses you have for a particular application (Number of Permanent Licenses) and the number of different computers on which you have discovered that application (Number of Permanent Licenses in Use). You are out of compliance if the number of permanent licenses in use exceeds the number of permanent licenses.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).

Parameter	How To Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

CompVersion

Use this Knowledge Script to generate a report detailing the version number of AppManager components installed on all computers in an AppManager site.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

CurrentDiskSpaceUsage

Use this Knowledge Script to generate a report detailing the used space on logical disks.

This report uses data collected by any Knowledge Script that monitors the available MB or the percentage of used space on a logical disk, such as NT_DiskSpace or UNIX_FileSystemSpace. Ensure you archive data detail when running the Knowledge Scripts to collect data. You must disable the *Do not archive data detail* option in the Advanced tab of the Knowledge Script properties dialog box to allow automatic data archiving.

Note
In the *Filter Settings* parameters, if you set the *Filter column* parameter to **Drive** and the *Filter operator* parameter to either **Greater than** or **Less than**, the script will not run but will raise an event indicating you made an invalid configuration of the script. For example, a drive can be equal to/not equal to C:, but not greater than/less than C:.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Select type	Select the method by which report content is ordered. Possible values are: • By computer • By drive • By total space • By space used • By percent used • By space free • By percent free For example, if you select By computer, then data is ordered by computer name. If you select By drive, data is ordered by drive letter.
Sort order	Select whether values are displayed in an ascending or descending order.
Filter Settings	

Parameter	How To Set It
Filter column	Use this parameter to set the first variable of the filtering equation. Use this parameter in conjunction with the *Select type* parameter. Make sure the two parameters have comparable values (for example, if *Select type* is set to *By drive*, set this parameter to *Drive*). If *Select type* is set to *By computer*, set this parameter to <*None*>. Possible values are: • <None> • Drive • Total space • Space used • Percent used • Space free • Percent free
Filter operator	Select an operator for the filtering equation. Possible values are: • Greater than • Less than • Equal to • Not equal to
Filter value	Specify a value for the second variable of the filtering equation. For example, if the first variable is *Drive*, and the operator is *Equal to*, set this parameter to *C:* to return data for all C: drives.
Report settings	
Disk space units	Select whether you would like the values in the report expressed in MB or GB.
Include parameter help card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. A job ID allows you to correlate a specific instance of a Report Script with the corresponding report. The default is unselected.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is Yes.
Event notification	
Event for report success?	Select **Yes** to raise an event when the report is successfully generated. The default is Yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).

Parameter	How To Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

DataStream

Use this Knowledge Script to generate a report containing high-level information about data streams collected by Knowledge Script jobs. High-level information includes the script names, data stream legends, and job IDs.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Select Knowledge Script(s)	Filter the data for your report by Knowledge Script.
Select job(s)	Filter the data for your report by specific Knowledge Script jobs.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID allows you to correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

DataSummary

Use this Knowledge Script to generate a report containing a statistical summary of selected data streams.

The data wizard allows you to select any combination of data streams for a report. Depending on which data streams you select and which style you select, your report can contain meaningful, easily-understood information, or it can contain information that is of no value.

The following examples of selecting data streams and report styles show the different types of information reports can contain in each case.

By computer style

If you select different data streams that use *different* units of measure, the report contains a separate value for each data stream from each computer.

For example, if you select the following data streams:

- `Ldsk: D:USED %`
- `Ldsk: D:AVAIL MB`

the report contains one value for each computer for the percentage of used space on the D: drive, and one value for each computer for the available megabytes on the D: drive.

If you select different data streams that use the *same* unit of measure, the report contains one value for each computer.

For example, if you select the following data streams:

- `Ldsk: D:USED %`
- `MemPhysUsage %`

the report contains a single percentage value for each computer. Each single percentage value is derived from all memory usage and disk usage values taken together. In this case, the values in the report are meaningless.

By legend style

If you select multiple data streams with the same legend from two different computers, the report contains one value for each different legend.

For example, if you select the following data streams:

- `Ldsk: D:USED %`
- `Ldsk: D:AVAIL MB`

the report contains one value for the percentage of used space on both D: drives, and one value for the available megabytes on both D: drives. This type of report would be useful, for example, if you wanted an overall statistic of disk space availability or memory use for something like a server farm.

If you select multiple data streams with different legends, the report contains one value for each legend.

For example, if you select the following data streams:

- `Ldsk: D:USED %`

- `MemPhysUsage %`

the report contains a single percentage value for each legend. One percentage value is derived from disk usage on both computers, the other from memory usage on both computers. As in the previous example, this type of report is useful for overall statistics.

By computer and legend style

The *by computer and legend* style lets you get individual values for each data stream from each computer.

Using this style, if you select the following data streams:

- `Ldsk: D:USED %`
- `Ldsk: D:AVAIL MB`

the report contains one value for each data stream for each computer.

If you select the following data streams:

- `MemPhysUsage %`
- `Ldsk: D:USED %`

the report contains one value for each data stream for each computer.

Regardless of the style you select, the table in the report always shows the average, minimum, maximum, and count values for a data stream. It may show additional values, as well, depending on how you configure the report.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Select peak weekday(s)	Filter the data for your report by days of the week.
Select the style	Select the style for the report: • **By computer** shows values for each computer you selected. • **By legend** shows one value for each different legend. • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	

Parameter	How To Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval (for example, the average value for 1 Hour) • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the aggregation interval • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the aggregation interval • **Close**: The last value for the aggregation interval • **Change**: The difference between the first and last values for the aggregation interval (close - open = change) • **Count**: The number of data points for the aggregation interval
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to yes, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to yes, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.

Parameter	How To Set It
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to yes to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to yes to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

DeletedObjects

Use this Knowledge Script to generate a report about objects that have been permanently deleted from the Operator Console TreeView. These are objects that have been deleted with the **Do not rediscover** option.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

DetailData

Use this Knowledge Script to generate a report containing information returned by Knowledge Scripts that prepare data for presentation in an XML format. If the data is not in an XML format, use the PlainDataInfo script.

You can use this report for any script that collects and displays data details in an XML format.

In order to have detail data available for this report, the *Collect data details with data point* option must be set in one of the following ways:

- for each relevant AppManager repository **(File > Preferences > Repository tab > Knowledge Script options > Advanced Properties)**
- on the Advanced properties tab of any individual Knowledge Script for which you want to generate a report.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select Knowledge Script	Filter the data for your report by Knowledge Script. If you have not collected data using a supported Knowledge Scripts, the browser is blank. If you change the name of a Knowledge Script, the new name appears in the browser.
Select computer(s)	Filter the data for your report by computer.
Select time range	Filter the data for your for report by a specific or sliding time range. The default is Sliding.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. A job ID helps you correlate a specific instance of a Report Script with the corresponding report.
Select properties	Set miscellaneous report properties as desired.

Parameter	How To Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. The default is n. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

DFSSummary

Use this Knowledge Script to generate a report containing details of the Distributed File System (DFS) service on specified computers. Details include the image path and services upon which DFS depends.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data in your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

EventArchiveSummary

Use this Knowledge Script to generate a report containing a summary of events per computer. The summary includes event IDs and statuses, Knowledge Scripts that raised the events, and event messages. The data for this report is taken from the ArchiveEvent table in the AppManager repository, which contains any archived event information you saved according to your AppManager repository preferences.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computers	Filter the data for your report by computer.
Select Knowledge Scripts	Filter the data for your report by Knowledge Script. The default is All.
Select jobs	Filter the data for your report by a specific Knowledge Script job. The default is All.
Event status	Filter the data for your report by event status. The default is All.
Select time range for last occurrence	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Report settings	
Limit the size of event detail	Specify the maximum number of characters to display in the event detail message. The default is 200.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder. The default folder name is ArchivedEventSummary.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired. The default report name is Archived Event Summary.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	

Parameter	How To Set It
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

EventSeveritySummary

Use this Knowledge Script to generate a report containing the number and severity of events raised by Knowledge Script jobs on specified computers.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

EventStatisticsSummary

Use this Knowledge Script to generate a report summarizing events per computer. Events are listed by monitored application. The total event count for each application is listed, as well as the count for each event status: open, acknowledged, closed.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

EventSummary

Use this Knowledge Script to generate a report containing a summary of events per computer. The summary includes event IDs and statuses, names of the Knowledge Scripts that raised the events, and event messages.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Select Knowledge Script(s)	Filter the data for your report by Knowledge Script.
Select job(s)	Filter the data for your report by specific Knowledge Script jobs.
Event status	Filter the data for your report by event status.
Select time range for last occurrence	Filter the data for your report by a specific or sliding time range. If the last occurrence of the event does not fall within this range, the report will have no data. The default is Sliding.
Report settings	
Limits the size of event detail	Specify the maximum number of characters to display in the event detail message. The default is 200.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.

Parameter	How To Set It
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

FRSSummary

Use this Knowledge Script to generate a report containing details of the File Replication Service (FRS) on specified computers. Details include image path and services upon which FRS depends.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

GeneralCounter

Use this Knowledge Script to generate a report containing a chart and table showing the average, maximum or minimum value of each selected data stream.

This report allows you to set the maximum number of data points illustrated in the chart, regardless of the number of data points that have been collected. For example, you may be collecting data every five minutes, but you want to report on the daily maximum value for the last week. Set the time range to 7 days, and set the maximum number of points per chart to 7. The report aggregates the data in increments of one day, and the chart illustrates seven maximum values for each selected data stream. The table in the report mirrors the chart settings: in this case, the table has seven rows of data.

The number of points in the chart do not have to correspond exactly to the time period on which you are reporting. You can illustrate a year's worth of data using 50 or 100 points, and you can illustrate a day's worth of data using 50 or 100 points. This script aggregates the data in the report according to the time range and points per chart settings.

This feature is useful for illustrating any time period in a single chart.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **By Knowledge Script** provides links to pages showing all data streams collected by a Knowledge Script (each page shows all data streams collected from all computers on which the script has run) • **All data streams on one page** generates a report with all data on a single page
Select time range	Filter the data for your report by a specific or sliding time range.
Select peak weekday(s)	Filter the data for your report by days of the week.

Parameter	How To Set It
Maximum number of points per chart	Specify the maximum number of data points illustrated in the chart. The default is 200. Possible values range from 5 to 1000.
Select average, minimum or maximum	Select the type of value you want in the report.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

GeneralMachineDown

Use this Knowledge Script to generate a report about computers that were detected as down during a specified time period.

This report uses data collected by the UNIX_PingMachine and General_MachineDown Knowledge Scripts.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer. **Note** You must select the computers on which the UNIX_PingMachine or General_MachineDown Knowledge Scripts were run.
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).

Parameter	How To Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

GroupPolicySummary

Use this Knowledge Script to summarize Group Policy settings for specified computers.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Inventory

Use this Knowledge Script to generate a report containing details of a specified application on a computer, including version number, root directory and security settings, or all components of a computer, including memory and disk configuration, and details of any applications monitored by AppManager.

This report contains information from a single AppManager repository.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select application	Select the application that is the subject of your report. Select **All Components** to report on all applications on specified computers.
Select computer(s)	Filter the data for your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).

Parameter	How To Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

JobInfo

Use this Knowledge Script to generate a report containing the details of Knowledge Script jobs.

The first page of the report lists the specified jobs by computer, and gives the job ID and status of each job. The job IDs are links to pages containing further details about each job. Details include the schedule for each job and the parameter settings.

Note
Run this script only on a management server computer.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Select job status	Filter the data for your report by job status.
Select job(s) (optional)	Filter the data for your report by specific Knowledge Script jobs. **Note** If you enable this parameter, do not enable the next parameter. You cannot successfully implement both optional parameters.
Select Knowledge Script(s) (optional)	Filter the data for your report by Knowledge Script. **Note** If you enable this parameter. You cannot successfully implement both optional parameters.
Sort by	Select a sorting method for the contents of the first page of the report: • **Computer** sorts the contents alphabetically by computer name • **Job ID** sorts the information for each computer numerically by job ID • **Knowledge Script Name** sorts the information for each computer alphabetically by Knowledge Script name • **Job Status** sorts the information for each computer alphabetically by job status
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.

Parameter	How To Set It
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

JobSummary

Use this Knowledge Script to generate a report about the Knowledge Script jobs, monitoring policies, actions, and events associated with each computer you are monitoring. The report includes all computers in a given AppManager repository.

The first page of the report lists each computer followed by the number of Knowledge Script jobs, monitoring policies, actions, and events associated with that computer. The computer names are links to pages containing further details about each Knowledge Script job on that computer. These details include:

- The job ID
- The Knowledge Script name
- The names of Knowledge Script Groups that include the Knowledge Script
- The names of any Action Knowledge Scripts initiated by the Knowledge Script job
- The number of events raised by the Knowledge Script job

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as desired.

Parameter	How To Set It
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

LastDataPoint

Use this Knowledge Script to generate a report about the value of the most recently collected data point in a data stream.

This report is useful for monitoring conditions such as database size or disk space; conditions where the current state of affairs is of most interest.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By Knowledge Script** provides links to pages showing all data streams collected by a Knowledge Script (each page shows all data streams collected from all computers on which the script has run) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer)
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder.

Parameter	How To Set It
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

ModuleUsage

Use this Knowledge Script to generate a report about the number of different AppManager modules in use (for example, the number of different SQL Servers on which you are running Knowledge Script jobs). The report contains:

- The module name
- The number of module licenses required
- The number of modules in use

You can use this report in conjunction with the CompLic Knowledge Script to identify differences between the number of module licenses and the number of modules deployed.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).

Parameter	How To Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

NetworkInterface

Use this Knowledge Script to generate a report detailing the network interface components on specified computers. Details include the manufacturer, IP address, and subnet mask.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

NTLogicalDisk

Use this Knowledge Script to generate a report detailing the logical disks on specified computers. Details include file systems, and drive sizes (in MB).

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

NTPhysicalDisk

Use this Knowledge Script to generate a report detailing physical disks on specified computers. Details include disk sizes (in MB), cylinders per disk, and tracks per cylinder.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

PerfOverview

Use this Knowledge Script to generate a report containing a single average value for each selected data stream for a specified increment of time, for example, an average value derived from one hour's worth of data or 30 days' worth of data.

If you expect the data sets from which you are deriving values to exceed 1.5 GB, use PerfOverviewLD instead of this script.

A separate chart is generated for each selected data stream.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By Knowledge Script** provides links to pages showing all data streams collected by a Knowledge Script (each page shows all data streams collected from all computers on which the script has run)
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Select peak weekday(s)	Filter the data for your report by days of the week.
Aggregation by	Select the method by which data in the report is aggregated. The options are: • Minute • Hour • Day This parameter is used in conjunction with the following parameter. For example, if you choose to aggregate by day, then the following parameter determines how many days' worth of data are aggregated.

Parameter	How To Set It
Aggregation interval	Select the interval at which the data in your report is aggregated. This parameter is used in conjunction with the previous parameter. For example, if the **Aggregation by** parameter is set to **Day**, use this parameter to set the number of days by which data is aggregated (1 gives you a single value for one day's worth of data, 2 gives you a single value for two days' worth of data, and so on).
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

PerfOverviewLD

Use this Knowledge Script in place of PerfOverview when the data sets from which you are deriving values exceed the ADO (ActiveX Data Objects) limit of 1.5 GB. When data sets exceed this size limit, the report agent cannot process the data. Use this script to process data on the SQL Server managing the AppManager repository and return the aggregated value to the report agent.

The report contains a single average value for each selected data stream for a specified increment of time, for example, an average value derived from one month's worth of data or one year's worth of data.

A separate chart is generated for each selected data stream.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By Knowledge Script** provides links to pages showing all data streams collected by a Knowledge Script (each page shows all data streams collected from all computers on which the script has run)
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Select peak weekday(s)	Filter the data for your report by the days of the week.
Aggregation by	Select the method by which data in the report is aggregated. The options are: • Hour • Day This parameter is used in conjunction with the following parameter. For example, if you choose to aggregate by day, then the following parameter determines how many days' worth of data are aggregated.

Parameter	How To Set It
Aggregation interval	Select the interval at which the data in your report is aggregated. This parameter is used in conjunction with the previous parameter. For example, if the **Aggregation by** parameter is set to **Day**, use this parameter to set the number of days by which data is aggregated (1 gives you a single value for one day's worth of data, 2 gives you a single value for two days' worth of data, and so on).
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

PlainDataInfo

Use this Knowledge Script to generate a report listing the details of data points in specified data streams. Details include the data point value, and the time at which the data point was collected. If the data is presented using an XML format, use the DetailData Knowledge Script.

In order to have detail data available for this report, the *Collect data details with data point* parameter must be set in one of the following ways:

- for each relevant AppManager repository (**File > Preferences > Repository tab > Knowledge Script options > Advanced Properties**)
- on the Advanced properties tab of any individual Knowledge Script for which you want to generate a report.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select Knowledge Script	Filter the data for your report by Knowledge Script.
Data stream	Specify the legend of the data streams that you want to include in your report. To return all data streams, enter ALL.
Select computer(s)	Filter the data for your report by computer.
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.

Parameter	How To Set It
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

PrinterSummary

Use this Knowledge Script to generate a report detailing the printers and printer drivers installed on specified computers.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

SerLevAvailability

Use this Knowledge Script to generate a report detailing the percentage of time specified services were up or down.

This report uses data collected by the NT_ServiceDown and General_ServiceDown Knowledge Scripts. In order to have accurate data for this report, schedule these Knowledge Scripts to run every five minutes.

If you are using NT_ServiceDown, set the *Collect data?* parameter to **y**, and the *Collect data only on down?* parameter to **n**, so that you are always collecting data, rather than collecting data only when a service is down.

Uptime and downtime are calculated during scheduled maintenance. Ad hoc maintenance is considered as downtime, and is included in all calculations.

Note
This script expects a certain number of data points per time period based on the parameter settings of the Knowledge Script collecting data. If any data points are missing, the corresponding times are considered as downtime. For example, if a Knowledge Script is configured to collect 12 data points per hour, but only collects six, then one half hour is considered downtime. Data points may be missing, for example, if the Knowledge Script job was stopped and restarted, or if the agent was not running for that period.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select the style	Select the style for the first page of the report: • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Select peak weekday(s)	Filter the data for your report by the days of the week.
Aggregation interval	Select the time period by which the data in your report is aggregated: • Hourly • Daily • Weekly
Report settings	

Parameter	How To Set It
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

SQLDBInfo

Use this Knowledge Script to generate a report detailing the databases managed by SQL Servers on specified computers. Details include the database names and owners, and database and log sizes (in MB).

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

SystemUpTime

Use this Knowledge Script to generate a report detailing the uptime and downtime of monitored computers. Uptime and downtime are illustrated in hours and minutes, as well as the percentage of the monitoring interval during which a computer is running or not. For example, if during a 24-hour monitoring interval, the computer is running for 18 hours and not running for six hours, the uptime and downtimes are represented as:

- Uptime: 18 hours 0 minutes
- Downtime: 6 hours 0 minutes
- Uptime: 75%
- Downtime: 25%

This report uses data collected by the NT_SystemUpTime and UNIX_SystemUpTime Knowledge Scripts. In order to have accurate data for this report, schedule these Knowledge Scripts to run every 5 minutes.

Uptime and downtime are calculated during scheduled maintenance. Ad hoc maintenance is considered as downtime, and is included in all calculations.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Select the style	Select the style for the first page of the report: • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Select peak weekday(s)	Filter the data for your report by the days of the week.
Aggregation interval	Select the time period by which the data in your report is aggregated: • Hourly • Daily • Weekly
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.

Parameter	How To Set It
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

SystemUpTimePie

Use this Knowledge Script to generate a report detailing the uptime and downtime of monitored computers. This report illustrates uptime and downtime using a pie chart. You can enter a minimum threshold for uptime. Any values below the threshold are colored red in the table in the report.

Uptime and downtime are illustrated in hours and minutes, as well as the percentage of the monitoring interval during which a computer is running or not. For example, if during a 24-hour monitoring interval, the computer is running for 18 hours and not running for six hours, the uptime and downtime are represented as:

- Uptime: 18 hours 0 minutes
- Downtime: 6 hours 0 minutes
- Uptime: 75%
- Downtime: 25%

This report uses data collected by the NT_SystemUpTime and UNIX_SystemUpTime Knowledge Scripts. In order to have accurate data for this report, schedule these scripts to run every 5 minutes.

Uptime and downtime are calculated during scheduled maintenance. Ad hoc maintenance is considered as downtime, and is included in all calculations.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Select computer(s)	Filter the data for your report by computer.
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Select peak weekday(s)	Filter the data for your report by the days of the week.
Uptime threshold %	Specify a value for the minimum uptime threshold. Any value below this threshold is colored red in the table. Use any value less than 100. You can use decimals.
Report settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.

Parameter	How To Set It
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Chart width	Provide a value for the width in pixels of the pie chart image.
Chart height	Provide a value for the height in pixels of the pie chart image.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

WatchList

Use this Knowledge Script to generate a report detailing the top or bottom N computers, by number or percent, that generated the selected data streams.

Resource Object

Report agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data source	
Top or bottom	Select either **Top** or **Bottom** as a filtering criterion.
Number N	Set the value of the *Top or bottom* parameter (for example, top 5 or bottom 5).
Number or percent	Select whether the report defines the top or bottom N by number or percent (for example, top 5 or bottom 5 percent).
Top or bottom by	Select which type of data stream values take precedence in the report: • Average • Minimum • Maximum For example, if you are reporting on the Top 5 computers and you set this parameter to Average, then the top 5 computers with the highest average values for the selected data streams are included in the report. In this case, the maximum and minimum values are also included, but the average values are listed first in the table, and the average values are by default given a unique graphic style in the chart. The report always includes all three values for the sake of comparison, but the type of value you select for this parameter is given precedence in the report.
Select data wizard	Select the data for your report by Knowledge Script or by data stream.
Select the style	Select the style for the first page of the report: • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By Knowledge Script** provides links to pages showing all data streams collected by a Knowledge Script (each page shows all data streams collected from all computers on which the script has run)
Select time range	Filter the data for your report by a specific or sliding time range. The default is Sliding.
Select peak weekday(s)	Filter the data for your report by the days of the week.
Report settings	

Parameter	How To Set It
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table/chart/both?	Select the type of data stream values you want to include in the report: • **Table** (table only) • **Chart** (chart only) • **Both** (table and chart)
Select chart style	Define the graphic properties of the charts in your report.
Top/bottom N series style	Select the graphical style of the data series representing the top or bottom N data streams.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is n.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp contains the date and time the report was generated. A time stamp allows you to run consecutive iterations of the same report without overwriting previous output. The default is n.
Event notification	
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red level indicator).

Chapter 62
SharePoint Knowledge Scripts

AppManager for Microsoft Office SharePoint Server 2007 provides the following Knowledge Scripts to monitor Microsoft Office SharePoint Server 2007 on Microsoft Windows computers.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
BytesTransfer	Monitors the total number of bytes transferred per second to and from a Web application.
ConnectionsInterval	Monitors the number of Web application connections.
ContentManagementEventLog	Monitors the event log for Content Management error events generated by SharePoint.
DBSpaceUtil	Monitors the percentage of space utilized by the SharePoint content database.
GenericEventLog	Monitors the event log for generic error events generated by SharePoint.
HealthCheck	Monitors the operational status of active SharePoint services and Web applications.
InfoPathEventLog	Monitors the event log for InfoPath Forms error events generated by SharePoint.
IsolatedApps	Monitors the number of isolated applications in the SharePoint environment.
RecycleBinInfo	Monitors the Recycle Bin usage for all the Web applications running on the SharePoint Server.
Report_ServerUptime	Generates a report about the number of hours the SharePoint Server has been operational since the last reboot.
Report_SiteInfo	Generates a report about the date and space utilization information for each Web application on the SharePoint Server.
Report_SiteUsage	Generates a report that contains usage information about each Web application on the SharePoint Server.
Report_WebPartInfo	Generates a report about the status and availability of Web Parts used by the SharePoint Server.
ServerUptime	Monitors the number of hours the SharePoint Server has been operational since the last reboot.
ServiceUptime	Monitors the uptime of Web applications on the SharePoint Server.
SiteEventLog	Monitors the event log for events on the Web application usage.

Knowledge Script	What It Does
SiteInfo	Monitors date and space utilization information for each Web application on the SharePoint Server.
SiteUsage	Monitors usage information about each Web application on the SharePoint Server.
WebPagePerf	Monitors the availability and performance of a Web application's Web pages on the SharePoint Server.
WebPartInfo	Monitors the status and availability of Web Parts used by the SharePoint Server.

BytesTransfer

Use this Knowledge Script to monitor the total number of bytes transferred per second to and from a Web application. This script raises an event if the total number of transferred bytes exceeds the threshold you set.

Resource Objects

SharePoint Server: Virtual Server and Virtual Server icon.

Default Schedule

The default interval for this script is every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if number of bytes transferred per second exceeds a threshold?	Select **Yes** to raise an event if the number of bytes transferred per second exceeds the threshold you specify. The default is Yes.
Event severity when the number of bytes transferred exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of bytes send or received exceeds the threshold you set. The default is 10.
Collect data for current transfer rate?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns byte transfer rate (sent and received) data for the server. The default is unselected.
Threshold -- Maximum bytes received per second	Specify the maximum number of bytes the server can receive before an event is raised. The default is 64000 bytes per second.
Threshold -- Maximum bytes sent per second	Specify the maximum number of bytes the server can send before an event is raised. The default is 64000 bytes per second.

ConnectionsInterval

Use this Knowledge Script to monitor the number of Web application connections and the total connections for all Web applications from anonymous and user (non-anonymous) accounts during the monitoring interval. This script raises an event if the number of connections exceeds the threshold you set.

Note
If anonymous access is not enabled for the Web applications in the SharePoint site collection, this script raises events only for maximum connections to Web applications from user (non-anonymous) accounts that exceed the threshold.

Resource Objects

SharePoint Server: Virtual Server and Virtual Server icon

Default Schedule

The default interval for this script is every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if number of connections exceeds any threshold?	Select **Yes** to raise an event if the number of connections exceeds the threshold you set. The default is Yes.
Event severity when current connections exceed the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of current connections exceed the threshold. The default is 12.
Collect data for number of connections?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of Web application connections during the monitoring interval is returned. The default is unselected.
Threshold -- Maximum connections to Web application from anonymous accounts	Specify the maximum number of Web application connections from anonymous accounts that can be open during the monitoring interval. An event is raised if the number of connections exceeds the threshold.The default is 64.
Threshold -- Maximum connections to Web application from non-anonymous accounts	Specify the maximum number of Web application connections from non-anonymous (user) accounts that can be open during the monitoring interval. An event is raised if the number of connections exceeds the threshold. The default is 64.
Threshold -- Maximum total connections to Web server from anonymous accounts	Specify the maximum total connections to all monitored Web applications from anonymous accounts that can be open during the monitoring interval. An event is raised if the number of connections exceeds the threshold. The default is 64.
Threshold -- Maximum total connections to Web server from non-anonymous accounts	Specify the maximum total number of connections to all monitored Web applications from non-anonymous (user) accounts that can be open during the monitoring interval. An event is raised if the number of connections exceeds the threshold. The default is 64.

ContentManagementEventLog

Use this Knowledge Script to monitor the event log for Content Management error events generated by SharePoint.

This Knowledge Script raises events for the following error codes:

- **5322** - Content deployment job could not contact the destination server
- **5323** - The connection to the destination server was lost while transporting the deployment package created by the content deployment job
- **5325** - The content deployment job failed on the destination server during the import phase
- **5326** - The content deployment job failed on the source server during the export phase

Resource Objects

SharePoint Server

Default Schedule

The default interval for this script is every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if SharePoint generates a Content Management error event?	Select **Yes** to raise an AppManager event if SharePoint generates a Content Management error event in the event log. The default is Yes.
Event severity when SharePoint generates a Content Management error event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which SharePoint generates a Content Management error event in the event log. The default is 20.
Data Collection	
Collect data for the Content Management error event?	Select **Yes** to collect data for charts and reports. The default is unselected.
Events in past N hours	Set this parameter to control event checking for the first interval (after which checking is incremental): • **-1** lists all the existing entries • **N** lists events for the past n hours, such as 8 for the past 8 hours, or 50 for the past 50 hours • **0** lists only entries from this moment on, without listing any previous entries The default is 0.
Max number of entries per event report	Specify the maximum number of entries, from 1 to 100, to be recorded in each event's detail message. If this script finds more entries from the log than it can put into one event message, it will return multiple events to report all the outstanding entries in the log. The default is 30 entries.

DBSpaceUtil

Use this Knowledge Script to monitor the percentage of space used by a SharePoint content database. Space usage is measured as a percentage of the total database space available to the selected SharePoint content database. This script raises an event if the percentage of space used by a SharePoint content database exceeds the threshold you set.

Resource Objects

SharePoint Server: Database and Database icon

Default Schedule

The default interval for this script is every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if database space used exceeds threshold?	Select **Yes** to raise an event if the percentage of used database space exceeds the threshold you set. The default is Yes.
Event severity when the percentage of database space used exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of used database space exceeds the threshold you set. The default is 5.
Collect data for amount of database space used?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of space utilized by the SharePoint content database. The default is unselected.
Threshold -- Maximum percentage of database space used	Specify the maximum percentage of space the SharePoint content database can use before an event is raised. The default is 75%.

GenericEventLog

This Knowledge Script monitors the event log for generic error events created by SharePoint. The SharePoint administrator can configure the event types in the SharePoint Central Administration site.

This script raises events for the following error codes:

- **42** - Propagation failed to communicate with a query server
- **2438** - Crawler cannot read from registry
- **2462** - Failed to load word breaker
- **2483|2484** - Failed to load protocol handler
- **3353** - Backup failed due to insufficient permissions
- **4105|4106** - Master merge error
- **4127** - Failed to load index
- **4138** - Index is corrupt
- **7035** - Backup failed due to timer job failure
- **10038** - Query server removed from rotation

Resource Objects

SharePoint Server: Virtual Server and Virtual Server icon

Default Schedule

The default interval for this script is every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if SharePoint generates a generic error event?	Select **Yes** to raise an event if SharePoint generates a generic error event in the event log. The default is Yes.
Event severity when SharePoint generates an error event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which SharePoint generates an error event. The default is 20.
Data Collection	
Collect data for the generic error event?	Select **Yes** to collect data for charts and reports. The default is unselected.

Description	How to Set It
Events in past N hours	Set this parameter to control event checking for the first interval (after which checking is incremental): • **-1** lists all the existing entries • **N** lists events for the past n hours, such as 8 for the past 8 hours, or 50 for the past 50 hours • **0** lists only entries from this moment on, without listing any previous entries The default is 0.
Max number of entries per event report	Specify the maximum number of entries, from 1 to 100, that you want to be recorded in each event's detail message. If this script finds more entries from the log than it can put into one event message, it will return multiple events to report all the outstanding entries in the log. The default is 30 entries.

HealthCheck

Use this Knowledge Script to monitor the operational status of active SharePoint services and Web applications. This script checks the status of all SharePoint services and sites on the SharePoint Server, and it can start a stopped service or site.

This script raises events if a service or site stops, fails to start, or stops and then starts again. This script also monitors the queue length for blocked I/O requests. In addition, this script generates data streams for service or site availability.

Resource Objects

SharePoint Server: Services (Windows services), SharePoint Services, and Virtual Server

Default Schedule

The default interval is every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HealthCheck job fails. The default is 5.
Monitor Services	
Start service or site if it is stopped?	Select **Yes** to automatically start all stopped services or sites on the SharePoint Server. The default is Yes. **Notes** • Only activated services can be automatically started. If an administrator has deactivated a service, then AppManager cannot start it. • The HealthCheck script will only start services that have a startup type of **Automatic**.
Event Notification	
Raise event if service or site is stopped and should not be started?	Select **Yes** to raise an event if a monitored service or site is stopped but you did not enable the *Start service or site if it is stopped* parameter. The default is Yes.
Event severity when service or site is stopped and should not be started	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service or site is stopped but you did not enable the *Start service or site if it is stopped* parameter. The default is 15.
Raise event if service or site fails to start?	Select **Yes** to raise an event if AppManager cannot start a monitored service or site. The default is Yes.
Event severity when service or site fails to start	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot start a monitored service. The default is 5.
Raise event if stopped service or site has been started?	Select **Yes** to raise an event if a service or site has been started since the last time this script ran. The default is Yes.

Description	How to Set It
Event severity when stopped service or site has been started	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service or site has been started since the last time this script ran. The default is 25
Raise event if threshold crossed for blocked I/O requests?	Select **Yes** to raise an event if the number of blocked I/O requests that can be in queue for a site or service exceeds the threshold you set. The default is unselected.
Threshold -- Maximum blocked I/O requests	Specify the maximum number of blocked I/O requests that can be in a queue before an event is raised.The default is 0 requests.
Event severity when blocked I/O requests exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of blocked I/O requests in queue exceeds the threshold. The default is 5.
Data Collection	
Collect data for service or site availability?	Select **Yes** to collect data for SharePoint services and site availability. The default is Yes.

InfoPathEventLog

Use this Knowledge Script to monitor the event log for InfoPath Forms error events generated by SharePoint. This script raises events for the following error codes:

- **5338** - InfoPath Forms Services calculations exceeded the maximum limit
- **5339** - InfoPath Forms Services rules exceeded the maximum limit
- **5340** - InfoPath Forms Services business logic exceeded the maximum limit of operations
- **5341** - InfoPath Forms Services was running business logic when ASP.NET request timed out
- **5342** - A form template's business logic caused an OutOfMemory exception
- **5343** - InfoPath Forms Services business logic exception occurred while loading a form template
- **5369** - InfoPath Forms Services cannot find or load ifsFileNames.xml
- **5374** - InfoPath Forms Services postback failure
- **5733** - InfoPath form templates have conflicting business logic assembly identities
- **5734** - InfoPath Forms Services business logic attempted to store a nonserializable object
- **5737** - InfoPath Forms Services user has exceeded the maximum number of actions per postback
- **5757** - InfoPath Forms Services found an unexpected session state version
- **5760** - InfoPath Forms Services event counter mismatch
- **7056** - InfoPath Forms Services failed to load a form template
- **7083** - InfoPath Forms Services user has exceeded the maximum session state size
- **7095** - The second stage Recycle bin has reached 90% capacity

Resource Objects

SharePoint Server

Default Schedule

The default interval for this script is every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if SharePoint generates an InfoPath Forms error event?	Select **Yes** to raise an event if SharePoint generates an InfoPath Forms error event in the event log. The default is Yes.
Event severity when SharePoint generates an InfoPath Forms error event	Set the event severity level, from 1 to 40, to indicate the importance of an event in which SharePoint generates an InfoPath Forms error event. The default is 20.
Data Collection	
Collect data for InfoPath Forms error events?	Select **Yes** to collect data to generate charts and reports for InfoPath Forms error events. The default is unselected.

Description	How to Set It
Events in past N hours	Set this parameter to control event checking for the first interval (after which checking is incremental): • **-1** lists all the existing entries • **N** lists events for the past n hours, such as 8 for the past 8 hours, or 50 for the past 50 hours • **0** lists only entries from this moment on, without listing any previous entries The default is 0.
Max number of entries per event report	Specify the maximum number of entries, from 1 to 100, that you want to be recorded in each event's detail message. If this script finds more entries from the log than it can put into one event message, it will return multiple events to report all the outstanding entries in the log. The default is 30 entries.

IsolatedApps

Use this Knowledge Script to monitor isolated applications in the SharePoint environment.

An "isolated" application is a stand-alone application that adds functionality to a SharePoint site, such as a third-party product created for use with SharePoint. An isolated application runs out-of-process, directly from the Web Server. Typically, an isolated application shares its resources with other components in that application.

The performance of SharePoint may be affected if several isolated applications run at the same time, and you can use this script to monitor the number of isolated applications to prevent this situation. This script raises an event if the number of isolated applications exceeds the threshold you set.

Resource Objects

SharePoint Server: Virtual Server and Virtual Server icon

Default Schedule

The default interval for this script is every 24 hours.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if number of isolated applications exceeds threshold?	Select **Yes** to raise an event if the number of isolated applications exceeds the threshold you set. The default is Yes.
Event severity when the number of isolated applications exceeds the threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which number of isolated applications exceeds the threshold you set. The default is 8.
Collect data for number of isolated applications?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of isolated applications. The default is unselected.
Threshold -- Maximum isolated applications	Specify the maximum number of isolated applications that are allowed before an event is raised. The default is 10.

RecycleBinInfo

Use this Knowledge Script to monitor Recycle Bin usage for all Web applications running on the SharePoint Server. This script raises an event if the percentage of the site quota for the Recycle Bin exceeds the specified threshold.

This script monitors two stages of Recycle Bins for site quota usage. By default, SharePoint Server enables the first, or primary, stage of the Recycle Bin. To monitor the secondary stage of the Recycle Bin, enable the secondary Recycle Bin. For more information about enabling the Recycle Bin features, see your Microsoft Office SharePoint Server documentation.

Note
This script works only if a quota has been defined for the site. The script does not work on Web applications and site collections that use the "No Quota" option. If no quotas are defined for a specific site, deselect the site from the Objects tab to avoid raising the extra events.

Resource Objects

SharePoint Server: Virtual Server and Virtual Server icon

Default Schedule

The default interval for this script is every 24 hours.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if first stage Recycle Bin site quota utilization exceeds threshold?	Select **Yes** to raise an event if the first stage Recycle Bin site quota exceeds the threshold you set. The default is Yes.
Threshold -- Maximum site quota utilization	Specify the maximum site quota utilization allowed before an event is raised. The default is 75%.
Event severity when site quota utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the first stage site quota usage threshold is exceeded. The default is 15.
Raise event if second stage Recycle Bin site quota exceeds threshold?	Select **Yes** to raise an event if the second stage Recycle Bin site quota exceeds the threshold you set. The default is Yes.
Threshold -- Maximum site quota utilization	Specify the maximum site quota utilization allowed before an event is raised. The default is 75%.
Event severity when site quota utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the second stage site quota usage threshold is exceeded. The default is 15.
Raise event if no data is available?	Select **Yes** to raise an event if no Recycle Bin information exists for the selected Web applications on the SharePoint Server. The default is unselected.
Event severity when no data is available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no Recycle Bin information exists. The default is 11.

Description	How to Set It
Data Collection	
Collect data for first stage Recycle Bin site quota utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns data for first stage Recycle Bin site quota use. The default is unselected.
Collect data for second stage Recycle Bin site quota utilization?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns data for second stage Recycle Bin site quota use. The default is unselected.

Report_ServerUptime

Use this Knowledge Script to summarize the number of hours the SharePoint Server has been operational since the last reboot. This report allows you to make a statistical analysis of the data point values.

This report uses data collected by the ServerUptime Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule is run once.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the day or days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select the statistical method to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Min/Avg/Max**: Minimum, average, and maximum values of data points for the time range of the report • **Range**: Range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: Measure of how widely values are dispersed from the mean • **Sum**: Total value of data points for the time range of the report • **Close**: Last value for the time range of the report • **Change**: Difference between the first and last values for the time range of the report (close - open = change) • **Count**: Number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N* % of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N* % of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percentage or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If you select **Yes**, then the data table shows only the top or bottom *N* or % (for example, only the top 10%). Otherwise, the table shows all data. The default is unselected.
Show totals on the table?	If you select **Yes**, additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: Average of all values in a column • **Report Minimum**: Minimum value in a column • **Report Maximum**: Maximum value in a column • **Report Total**: Total of all values in a column The default is unselected.
Report settings	
Include parameter help card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include table?	Select **Yes** to include a table of data stream values in the report. The default is Yes.
Include chart?	Select **Yes** to include a chart of data stream values in the report. The default is Yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script and the corresponding report. The default is unselected.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is unselected.
Event notification	
Event for report success?	Select **Yes** to raise an event in which the report is successfully generated. The default is Yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5.

Report_SiteInfo

Use this Knowledge Script to summarize information about the Web applications on the SharePoint Server, sorted by date and space utilized. This report allows you to make a statistical analysis of the data point values.

This report uses data collected by the SiteInfo Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule is run once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data source	
Select computerwizard	Select the computers for your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By data stream** shows one value for each different legend on the report • **By computer and data stream** shows one value for each unique legend from each computer. • **By Knowledge Script** shows values based on this Knowledge Script. • **All data streams on one page** shows values of all data streams on a single page.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select an aggregation method by which to display data in the report: • **Minute:** Average values based on minutes. • **Hour:** Average values based on hours. • **Day**: Average values based on days. The default is **Hour**.
Aggregation interval	Select an aggregation interval by which to display data in the report. You can select an aggregation interval in the range of 1 through 90. Data in the report is displayed based both on the aggregation method and interval. For example, 90 hours, 24 minutes, 7 days.

Parameter	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Count**: Number of data points for the time range of the report • **Sum**: Total value of data points for the time range of the report • **3Sigma:** The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**: Measure of how widely values are dispersed from the mean. • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**: The first value for the aggregation interval. • **Close**: Last value for the time range of the report.
Report settings	
Include parameter help card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include table?	Select **Yes** to include a table of data stream values in the report. The default is Yes.
Include chart?	Select **Yes** to include a chart of data stream values in the report. The default is Yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script and the corresponding report. The default is unselected.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is unselected.
Event notification	
Event for report success?	Select **Yes** to raise an event in which the report is successfully generated. The default is Yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5.

Report_SiteUsage

Use this Knowledge Script to summarize usage information about each Web application on the Microsoft Office SharePoint Server. This report allows you to make a statistical analysis of the data point values.

This report uses data collected by the SiteUsage Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule is run once.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computerwizard	Select the computers for your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By data stream** shows one value for each different legend on the report • **By computer and data stream** shows one value for each unique legend from each computer. • **By Knowledge Script** shows values based on this Knowledge Script. • **All data streams on one page** shows values of all data streams on a single page.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select an aggregation method by which to display data in the report: • **Minute:** Average values based on minutes. • **Hour:** Average values based on hours. • **Day**: Average values based on days. The default is **Hour**.
Aggregation interval	Select an aggregation interval by which to display data in the report. You can select an aggregation interval in the range of 1 through 90. Data in the report is displayed based both on the aggregation method and interval. For example, 90 hours, 24 minutes, 7 days.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Count**: Number of data points for the time range of the report • **Sum**: Total value of data points for the time range of the report • **3Sigma:** The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**: Measure of how widely values are dispersed from the mean. • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**: The first value for the aggregation interval. • **Close**: Last value for the time range of the report.
Report settings	
Include parameter help card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include table?	Select **Yes** to include a table of data stream values in the report. The default is Yes.
Include chart?	Select **Yes** to include a chart of data stream values in the report. The default is Yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script and the corresponding report. The default is unselected.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is unselected.
Event Notification	
Event for report success?	Select **Yes** to raise an event in which the report is successfully generated. The default is Yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5.

Report_WebPartInfo

Use this Knowledge Script to summarize the status and availability of Web Parts used by the Microsoft Office SharePoint Server. This report allows you to make a statistical analysis of the data point values.

This report uses data collected by the WebPartInfo Knowledge Script.

Resource Object

Report agent

Default Schedule

The default schedule is run once.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer wizard	Select the computers for your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By data stream** shows one value for each different legend on the report • **By computer and data stream** shows one value for each unique legend from each computer. • **By Knowledge Script** shows values based on this Knowledge Script. • **All data streams on one page** shows values of all data streams on a single page.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select an aggregation method by which to display data in the report: • **Minute:** Average values based on minutes. • **Hour:** Average values based on hours. • **Day**: Average values based on days. The default is **Hour**.
Aggregation interval	Select an aggregation interval by which to display data in the report. You can select an aggregation interval in the range of 1 through 90. Data in the report is displayed based both on the aggregation method and interval. For example, 90 hours, 24 minutes, 7 days.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: Average value of data points for the time range of the report • **Minimum**: Minimum value of data points for the time range of the report • **Maximum**: Maximum value of data points for the time range of the report • **Count**: Number of data points for the time range of the report • **Sum**: Total value of data points for the time range of the report • **3Sigma:** The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**: Measure of how widely values are dispersed from the mean. • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**: The first value for the aggregation interval. • **Close**: Last value for the time range of the report.
Report settings	
Include parameter help card?	Select **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include table?	Select **Yes** to include a table of data stream values in the report. The default is Yes.
Include chart?	Select **Yes** to include a chart of data stream values in the report. The default is Yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Select **Yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script and the corresponding report. The default is unselected.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Select **Yes** to append a timestamp to the title of the report, making each title unique. The timestamp is composed of the date and time the report was generated. A timestamp lets you run consecutive iterations of the same report without overwriting previous output. The default is unselected.
Event Notification	
Event for report success?	Select **Yes** to raise an event in which the report is successfully generated. The default is Yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5.

ServerUptime

Use this Knowledge Script to monitor the number of hours the servers hosting the SharePoint Server have been operational since the last reboot, giving you real-time data about the availability of the SharePoint Server.

This script raises an event if servers hosting the SharePoint Server are rebooted during the monitoring interval.

Resource Object

SharePoint Server

Default Schedule

The default interval for this script is every 5 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise an event if a system is rebooted during the monitoring interval?	Select **Yes** to raise an event if a computer hosting the SharePoint Server is rebooted during the monitoring interval. The default is Yes.
Event severity when system is rebooted	Set the severity level, from 1 to 40, to indicate the importance of the event in which a system is rebooted during the monitoring interval. The default is 25.
Collect data for SharePoint Server reboot?	Select **Yes** to collect data about SharePoint Server reboot. The default is unselected.

ServiceUptime

Use this Knowledge Script to monitor the uptime of Web applications on your Microsoft Office SharePoint Server. *Uptime* is the minimum time (threshold) that Web applications on your Microsoft Office SharePoint Server should run. This script raises an event if uptime for Web applications falls below the threshold you set.

Resource Objects

SharePoint Server: Virtual Server and Virtual Server icon

Default Schedule

The default interval for this script is every hour.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if Web application uptime falls below threshold?	Select **Yes** to raise an event if the length of time a Web application has been running falls below the threshold you set. The default is Yes.
Event severity when uptime falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of the event if the Web application uptime falls below the threshold you set. The default is 5.
Collect data for Web application uptime?	Select **Yes** to collect data about Web application uptime. The default is unselected.
Threshold -- Minimum Web application uptime	Specify the minimum uptime that a Web application must maintain to prevent an event from being raised. The default is 10000 seconds.

SiteEventLog

Use this Knowledge Script to monitor the event log for events related to Web application usage on the SharePoint Server.

This script raises events for the following error codes:

- **642** - User Account Maintenance
- **5187** - My Web application Creation failure
- **5550** - A Web application move operation has failed - leaving the Web application structure in an unusual state
- **5551** - A Web application copy operation has failed - leaving the Web application structure in an unusual state
- **5552** - A Web application deletion operation has failed - leaving the Web application structure in an unusual state
- **5553** - Web application Synch failed
- **5555** - Content Database Synchronization failed
- **5707** - Profile Import Failed
- **5708** - Membership Import failed

Resource Objects

SharePoint Server

Default Schedule

The default interval for this script is every 10 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if the Web application raises an error?	Select **Yes** to raise an event if the Web application raises an error event in the event log. The default is Yes.
Event severity when an event is raised	Set the event severity level, from 1 to 40, to indicate the importance of an event raised as a result of an error event in the event log. The default is 20.
Data Collection	
Collect data for site event log?	Select **Yes** to collect data for charts and reports. The default is unselected.

Description	How to Set It
Events in past N hours	Set this parameter to control event checking for the first interval (after which checking is incremental): • **-1** lists all the existing entries • **N** lists events for the past n hours, such as 8 for the past 8 hours, or 50 for the past 50 hours • **0** lists only entries from this moment on, without listing any previous entries The default is 0.
Max number of entries per event report	Specify the maximum number of entries, from 1 to 100, that you want to be recorded in each event's detail message. If this script finds more entries from the log than it can put into one event message, it will return multiple events to report all the outstanding entries in the log. The default is 30 entries.

SiteInfo

Use this Knowledge Script to monitor date and space utilization information about the Web applications on the SharePoint Server. The date information refers to when the file was last modified, and the space information refers to the size of the file.

Space utilization information includes the number of Web applications that have been added recently, along with the number of existing Web applications that have been modified, and Web applications that have been deleted. You can obtain detailed information about SharePoint Web application types such as documents, document libraries, and lists in report format.

This script helps you quickly locate the Web applications that are using more than the maximum amount of allotted space. The script raises an event if date or space utilization exceeds the threshold you set.

Web application information is displayed in report format, which you can customize.

Resource Objects

SharePoint Server: Virtual Server and Virtual Server icon

Default Schedule

The default interval for this script is every 24 hours.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Site Information	
Collect data for date information about Web applications?	Select **Yes** to collect date information, such as when Web applications were created, and last modified. The default is Yes.
Collect data for space utilization information for Web applications?	Select **Yes** to collect information about space utilized by each Web application on the SharePoint Server. The default is Yes.
Event Notification	
Raise event for date information?	Select **Yes** to raise an event in which the Knowledge Script collects date information for Web applications on the SharePoint Server. The default is Yes.
Event severity when site date information is collected successfully	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Web application date information is successfully collected. The default is 25.
Raise event for space utilization?	Select **Yes** to raise an event in which the Knowledge Script collects space utilization information for Web applications on the SharePoint Server. The default is Yes.
Event severity when space utilization data is collected successfully	Set the event severity level, from 1 to 40, to indicate the importance of an event in which space utilization information about Web applications is successfully collected. The default is 25.
Raise event if no data is available?	Select **Yes** to raise an event if no date or space utilization information exists for the Web applications on the SharePoint Server. The default is unselected.
Event severity when no data is available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no date or space utilization information exists. The default is 11.

Description	How to Set It
Data Collection	
Collect site date information?	Select **Yes** to collect site date information. If enabled, data collection returns information about the date that sites were created and last modified. The default is Yes.
Collect site space utilization data?	Select **Yes** to collect information about space utilized by each site on the SharePoint Server. If enabled, data collection returns information about how much space each site utilizes. The default is Yes.
Monitoring	
Enter date in the format mm/dd/yyyy	To monitor date information, such as when a file was last modified, specify the date in the following format: `mm/dd/yyyy` If you alter the date format, the report displays an error. The default is blank.
Select site type:	Select the type of SharePoint Web application that you want to view in the report. This Knowledge Script identifies Web application types using codes. Select: • **0-All:** to view all Web application types in the report • **1-Lists**: to view only the “lists” Web application type in the report • **2-Document Library**: to view only the “document library” Web application type in the report • **3-Document:** to view only the “documents” Web application type in the report. If you do not select a specific Web application type, all Web application types are displayed in the report by default.
Threshold -- Maximum KB of space utilized by each site	Specify the maximum amount of space that can be used by Web applications before an event is raised. The default is 0 KB.
Display report in ascending order?	Select **Yes** to view the report items in the ascending order of the items’ last modified date. The default is unselected.
The maximum number of records to display.	Specify the maximum number of records you want to return in your report. If you set the number to 0, then all of the records will be returned. If you set the number to 10, then only the ten top records will be returned. The default is 50.

SiteUsage

Use this Knowledge Script to monitor usage information about each Web application on the Microsoft Office SharePoint Server.

This script collects usage information based on the following parameters:

- URL
- User
- Operating System
- Browser
- Referrer URL

Web application usage information is displayed in report format. You can customize the format in which information is displayed in the report.

Resource Objects

SharePoint Server: Virtual Server and Virtual Server icon

Default Schedule

The default interval for this script is every hour.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event when report of site usage is created?	Select **Yes** to raise an event in which a report for Web application usage information is generated. The default is Yes.
Event severity when site usage data collection is successful	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Web application usage data is successfully collected. The default is 25.
Raise event if no data is available?	Select **Yes** to raise an event if no usage information exists for the Web applications on the SharePoint Server. The default is unselected.
Event severity when no data is available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no usage information exists. The default is 11.
Collect site usage data on the SharePoint server?	Select **Yes** to collect usage data for Web applications on your Microsoft Office SharePoint Server. The default is Yes.

Description	How to Set It
Select report type:	Select the report type that you want to view. The report type dictates how data is filtered (included or excluded). This script identifies report types using codes. Select the code to view the report based on that code. **0—URL**: URLs of pages that are visited, or of pages for lists that are updated. **1—User**: Names of users who visited the Web application. **2—OS**: The operating system used on the client computer. All Web application usage data refers specifically to visits from referrer URLs external to the application. **3—Browser**: The type of Web browser used to visit the SharePoint Web application. All usage data refers specifically to visits from referrer URLs external to the application. **4—RefURL**: External URLs through which users navigated to the SharePoint application. The default is 0—URL.
Select report format (past 31 days):	Select the format in which you want to view the report: **0—Day-wise**: Data is displayed individually for each day for the past 31 days. **1—Summary**: Data for the past 31 days is displayed as a summary. The default is 0-Day-wise.

WebPagePerf

Use this Knowledge Script to monitor the performance of Web pages in a SharePoint Web application.

This script retrieves performance information by scanning the SharePoint log entries. The script uses the current date's log file to retrieve the performance information. The script uses the Usage Analysis Logs found in the following folder:

```
\Program Files\Common Files\Microsoft Shared\Web server extensions\12\LOGS\guid
of Webpp\
```

Performance is measured in terms of the bandwidth you specify. Bandwidth is the number of bytes transferred to and from Web applications. This script raises an event if a log entry exceeds the bandwidth threshold you set.

Resource Objects

SharePoint Server: Virtual Server and Virtual Server icon

Default Schedule

The default interval for this script is every 24 hours.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if log entries exceed the bandwidth threshold?	Select **Yes** to raise an event in which log entries exceed the bandwidth threshold you specify. The default is Yes.
Event severity when bandwidth exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the bandwidth exceeds the threshold. The default is 8.
Raise event if no data is available?	Select **Yes** to raise an event if no bandwidth information exists for the Web page on the SharePoint Server. The default is unselected.
Event severity when no data is available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no bandwidth information exists. The default is 11.
Threshold -- maximum bandwidth	Specify the maximum bandwidth allowed before an event is raised. This script supports a maximum bandwidth of 4096 MB. The default is 1 MB.
Collect data for matching log entries?	Select **Yes** to collect data for charts and reports. The default is unselected.

WebPartInfo

Use this Knowledge Script to monitor the status and availability of Web Parts used by the SharePoint Server.

A *Web Part* is a modular unit of information located within the SharePoint site collection. A typical example of a Web Part is a digital dashboard on your company's SharePoint site collection, which integrates numerous information sources, enterprise applications, and other resources on a single page.

This script raises an event when it collects information about Web Parts and displays it in report format.

Resource Objects

SharePoint Server: Virtual Server and Virtual Server icon

Default Schedule

The default interval for this script is every 30 minutes.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event when details of Web Parts are collected?	Select **Yes** to raise an event in which details of Web Parts used by the SharePoint Server are collected. The default is Yes.
Event severity when data collection for Web Parts is successful	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Web Part details are successfully collected. The default is 25.
Raise event if no data is available?	Select **Yes** to raise an event if no Web Part information exists for the selected object on the SharePoint Server. The default is unselected.
Event severity when no data is available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no Web Part information exists. The default is 11.
Collect data for Web Parts on the SharePoint Server?	Select **Yes** to collect data points for all Web Parts on the SharePoint site collection. The default is Yes.

Chapter 63
Siemens ServerView Knowledge Scripts

The Siemens category provides the following Knowledge Scripts for monitoring Siemens PRIMERGY servers running ServerView. To access more information about any Knowledge Script, select the Knowledge Script and click **Help** in the Knowledge Script view of Control Center. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AdaptecLogicalDriveStatus	Monitors the status of logical drives on an Adaptec RAID controller.
AdaptecPhysicalDiskStatus	Monitors the status of physical disks on an Adaptec RAID controller.
AdaptecRAIDControllerStatus	Monitors the status of Adaptec RAID controllers and any attached hard drives.
ArrayLogicalDriveStatus	Monitors the status of a logical drive on a MYLEX RAID controller.
ArrayPhysicalDiskHardErrors	Monitors the number of hardware errors on a disk connected to a MYLEX RAID controller.
ArrayPhysicalDiskMiscErrors	Monitors the number of miscellaneous errors on a disk connected to a MYLEX RAID controller.
ArrayPhysicalDiskParityErrors	Monitors the number of parity errors on a disk connected to a MYLEX RAID controller.
ArrayPhysicalDiskSoftErrors	Monitors the number of software errors on a disk connected to a MYLEX RAID controller.
ArrayPhysicalDiskStatus	Monitors the status of a disk connected to a MYLEX RAID controller.
CPU	Monitors the status of one or more CPUs.
Fan	Monitors the status of individual fans.
HealthCheck	Monitors ServerView-related services.
IDEPhysicalDevice	Monitors discovered IDE physical devices, such as disk or CD-ROM devices.
LSILogicalDriveHealth	Monitors the physical device status, errors, and S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) status.
LSIPhysicalDeviceHealth	Monitors physical disk status.
MemoryModule	Monitors the status of memory modules on the system board.
NICError	Monitors the network interface card for transmission errors.
NICFail	Checks the status of the network interface card.
OverallCondition	Monitors the overall condition of discovered subsystems, for example, mass storage, system board, power supply, and environment.

Knowledge Script	What It Does
PowerSupply	Monitors the status of one or more internal power supply units.
SCSIPhysicalDevice	Monitors discovered SCSI physical devices, such as disk or CD-ROM devices.
Temperature	Monitors the server's thermal environment and the status of the server's temperature sensors.
Voltage	Monitors the voltage levels found on the system board.

AdaptecLogicalDriveStatus

Use this Knowledge Script to monitor the status of logical drives on an Adaptec RAID controller. This Knowledge Script raises an event if the logical drive is degraded, building, rebuilding, or has failed.

This Knowledge Script also raises an event if the status of the drive is `other`, which includes invalid, verifying, formatting, formatCertifying, notCreated, verifyingFixing, abortActivity, and reserved.

In addition, the Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

Adaptec Logical Drive folder or Adaptec Logical Drive icon.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the logical drive is operating properly • **50** if the logical drive is degraded, building, or rebuilding (this value is also returned to indicate a status of `other`) • **0** if the logical drive has failed The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...logical drive failed**. The default is 5 (red event indicator). • **...logical drive degraded**. The default is 15 (yellow event indicator). • **...logical drive building or rebuilding**. The default is 20 (yellow event indicator). • **...logical drive at other status**. The default is 20 (yellow event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

AdaptecPhysicalDiskStatus

Use this Knowledge Script to monitor the status of physical disks on an Adaptec RAID controller. This Knowledge Script raises an event if the disk is building, rebuilding, has issued a warning, or has failed.

The Knowledge Script also raises an event if the status of the disk is `other`, which includes invalid, verifying, formatting, formatCertifying, notCreated, verifyingFixing, abortActivity, and reserved.

In addition, the Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

Adaptec Physical Disk folder or Adaptec Physical Disk icon.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the physical disk is operating properly • **50** if the physical disk has issued a warning, is building, or rebuilding (this value is also returned to indicate a status of `other`) • **0** if the physical disk has failed or is missing The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...physical disk failed or missing**. The default is 5 (red event indicator). • **...physical disk degraded or warning**. The default is 15 (yellow event indicator). • **...physical disk building or rebuilding**. The default is 20 (yellow event indicator). • **...physical disk at other status**. The default is 20 (yellow event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

AdaptecRAIDControllerStatus

Use this Knowledge Script to monitor the status of Adaptec RAID controllers and any attached hard drives. This Knowledge Script raises an event if the controller or an attached hard drive has failed or issued an error.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

Adaptec RAID Controller folder or Adaptec RAID Controller icon.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the controller and attached drives are operating properly • **50** if the controller or an attached drive has issued an error • **0** if the controller or an attached drive has failed, is invalid, or is not supported The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...RAID Controller failed**. The default is 5 (red event indicator). • **...RAID Controller error**. The default is 15 (yellow event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

ArrayLogicalDriveStatus

Use this Knowledge Script to monitor the status of a logical drive on a MYLEX RAID controller. A *logical drive* is a combination of partitions on physical disks. If the logical drive status is dead or unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

Array Logical Drive folder or Array Logical Drive icon.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the logical drive is operating properly • **50** if the logical drive status is unknown • **0** if the logical drive is dead The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...logical drive critical**. The default is 5 (red event indicator). • **...logical drive offline or status unknown**. The default is 25 (blue event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

ArrayPhysicalDiskHardErrors

Use this Knowledge Script to monitor the status of the physical disks connected to a MYLEX RAID controller. If the number of hardware errors exceeds the threshold, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

If a disk experiences frequent hardware errors, replace the defective disk.

Resource Objects

Array Physical Disk folder or individual Array Physical Disk icon.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the number of hardware errors encountered by a physical disk. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Maximum threshold for hardware errors	Enter a threshold for the maximum number of hardware errors in a monitoring interval. The default is 5.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...threshold exceeded**. The default is 5 (red event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

ArrayPhysicalDiskMiscErrors

Use this Knowledge Script to monitor the status of the physical disks connected to a MYLEX RAID controller. If the number of miscellaneous errors exceeds the threshold, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

If a disk experiences frequent miscellaneous errors, replace the defective disk.

Resource Objects

Array Physical Disk folder or individual Array Physical Disk icon.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the number of miscellaneous errors encountered by a physical disk. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Maximum threshold for miscellaneous errors	Enter a threshold for the maximum number of miscellaneous errors in a monitoring interval. The default is 5.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...threshold exceeded**. The default is 5 (red event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

ArrayPhysicalDiskParityErrors

Use this Knowledge Script to monitor the status of the physical disks connected to a MYLEX RAID controller. At certain RAID levels, data blocks are protected by redundant data (so-called parity blocks). This Knowledge Script shows a count of the errors detected during this procedure.

If the number of parity errors exceeds the threshold, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

If a disk experiences frequent parity errors, check cabling and termination. This error may be caused by:

- Improper parity generation and checking
- Cable failure
- Improper cable length
- Improper or missing cable termination
- Interference from another device

Resource Objects

Array Physical Disk folder or individual Array Physical Disk icon.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the number of parity errors encountered by a physical disk. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Maximum threshold for parity errors	Specify the maximum number of parity errors that can occur during a monitoring interval before an event is raised. The default is 5.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...threshold exceeded**. The default is 5 (red event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

ArrayPhysicalDiskSoftErrors

Use this Knowledge Script to monitor the status of the physical disks connected to a MYLEX RAID controller. If the number of software errors exceeds the threshold, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

If a disk experiences a software error, run Siemens consistency check. If the disk experiences frequent software errors, replace the defective disk.

Resource Objects

Array Physical Disk folder or individual Array Physical Disk icon.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the number of software errors encountered by a physical disk. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Maximum threshold for software errors	Specify the maximum number of software errors that can occur during a monitoring interval before an event is raised. The default is 5.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...threshold exceeded**. The default is 5 (red event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

ArrayPhysicalDiskStatus

Use this Knowledge Script to monitor the status of the physical disks connected to a MYLEX RAID controller. If a disk is dead or its status is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

Array Physical Disk folder or individual Array Physical Disk icon.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the physical disk is operating properly • **50** if the physical disk status is rebuilding • **30** if the physical disk status is unknown • **0** if the physical disk is dead The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...physical disk dead** (the disk status is `dead`, the disk does not exist, the disk exists but is not powered on, the disk was deactivated by the controller due to an error). The default is 5 (red event indicator). • **...physical disk rebuilding**. The default is 18 (yellow event indicator). • **...physical disk status unknown**. The default is 25 (yellow event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

CPU

Use this Knowledge Script to monitor the status of one or more CPUs. If a CPU fails or its status is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

CPU Folder or individual CPU icons.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the CPU status is OK • **30** if the CPU status is unknown • **0** if the CPU is in any other state The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...CPU failed**. The default is 5 (red event indicator). • **...prefailure warnings**. The default is15 (yellow event indicator). • **...CPU status unknown**. The default is 25 (blue event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

Fan

Use this Knowledge Script to monitor the status of individual fans. If a fan is not operating properly or if its status is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

Fan Folder or individual Fan icons.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the fan status and speed. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...fan has failed**. The default is 5 (red event indicator). • **...fan failure predicted**. The default is15 (yellow event indicator). • **...redundant fan failed**. The default is 15 (yellow event indicator). • **...fan status is unknown**. The default is 25 (blue event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

HealthCheck

Use this Knowledge Script to monitor all ServerView-related services. If a ServerView-related service is not running, this Knowledge Script raises an event, performs the action you specify in the Actions tab of the Knowledge Script, and automatically restarts the service.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

In order for SNMP errors to generate an event, you need to run this Knowledge Script in the TreeView on an object at the Siemens Server level or above.

Resource Objects

Siemens Server or any Siemens Service icon.

Default Schedule

The default interval for this Knowledge Script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Auto-start service?	Set to **y** to automatically restart stopped services. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the status of ServerView-related services. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...service down; restart failed**. The default is 5 (red event indicator). • **...service down; restart succeeded**. The default is 25 (blue event indicator). • **...service down; don't restart**. The default is 18 (yellow event indicator). • **...SNMP down**. The default is 5 (red event indicator).

IDEPhysicalDevice

Use this Knowledge Script to monitor discovered IDE physical devices such as, disk or CD-ROM devices. If a device fails, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

IDE folder or individual IDE drives.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set it
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns 100 if the IDE device is operating properly or 0 if the IDE device is dead. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...IDE device failure**. The default is 5 (red event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

LSILogicalDriveHealth

Use this Knowledge Script to monitor logical drive status on LSI MegaRAID controllers. If the logical drive status is Rebuilding, Failed, Degraded, or Unknown, an event is raised.

Resource Objects

LSI Logical Drive folder or individual Logical Drive icon

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set it
General Settings	
Community string	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Job failure event notification	
Event severity for SNMP or ServerView service down	Set the severity level from 1 to 40 to indicate the importance on an event in which the SNMP or ServerView service is down. The default is 10.
Event Notification	
Status Settings	
Raise event when status of logical drive is Failed?	Select **Yes** to raise an event when the status of the logical drive is Failed. The default is Yes.
Event severity when status of logical drive is Failed	Set the severity level from 1 to 40 to indicate the importance of an event in which the status of the logical drive is Failed. The default is 5.
Raise event when status of logical drive is Degraded or Rebuilding	Select **Yes** to raise an event when the status of the logical drive is Degraded or Rebuilding. The default is Yes.
Event severity when status of logical drive is Degraded or Rebuilding	Set the severity level from 1 to 40 to indicate the importance of an event in which the status of the logical drive is Degraded or Rebuilding. The default is 18.
Raise event when status of logical drive is Unknown	Select **Yes** to raise an event when the status of the logical drive is Unknown. The default is unselected.
Event severity when status of logical drive is Unknown	Set the severity level from 1 to 40 to indicate the importance of an event in which the status of the logical drive is Unknown. The default is 35.
Data Collection	
Collect data for logical drive status?	Set to **Yes** to collect data for charts and reports. If set to Yes, this Knowledge Script records the operational status of the logical drive at each monitoring interval. The default is unselected.

LSIPhysicalDeviceHealth

Use this Knowledge Script to monitor physical device status, device errors, and S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) status on LSI Mega RAID controllers. If the physical device status is Rebuilding, Failed, or Unknown or if the number of errors exceed the threshold you set, an event is raised. An event is also raised if failure is predicted for a physical device or the S.M.A.R.T status is not known.

Resource Objects

Disk Array folder or LSI Physical Disk folder or individual Physical disk icon

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed

Parameter	How to Set it
General Settings	
community string name	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Job failure event notification	
Event severity for SNMP or ServerView service down	Set the severity level from 1 to 40 to indicate the importance on an event in which SNMP or the ServerView service is down. The default is 10.
Event Notification	
Status Settings	
Raise event when status of physical device is Rebuilding?	Select **Yes** to raise an event when the status of the physical device is Rebuilding. The default is Yes.
Event severity when status of physical device is Rebuilding	Set the severity level from 1 to 40 to indicate the importance of an event in which the status of the physical device is Rebuilding. The default is 15.
Raise event when status of physical device is Failed?	Select **Yes** to raise an event when the status of the physical device is Failed. The default is Yes.
Event severity when status of physical device is Failed	Set the severity level from 1 to 40 to indicate the importance of an event in which the status of the physical device is Failed. The default is 5.
Raise event when status of physical device is Unknown	Select **Yes** to raise an event when the status of the physical device is Unknown. The default is unselected.
Event severity when status of physical device is Unknown	Set the severity level from 1 to 40 to indicate the importance of an event in which the status of the physical device is Unknown. The default is 35.
S.M.A.R.T. Status Settings	
Raise event when failure is predicted for physical device?	Select **Yes** to raise an event when failure is predicted for the physical device. The default is Yes.

Parameter	How to Set it
Event severity when failure is predicted for physical device	Set the severity level from 1 to 40 to indicate the importance of an event in which failure is predicted for the physical device. The default is 15.
Raise event when S.M.A.R.T. Status of physical device is not available?	Select **Yes** to raise an event when the S.M.A.R.T. status for the physical device is not available. The default is unselected.
Event severity when S.M.A.R.T. Status of physical device is Not Available.	Set the severity level from 1 to 40 to indicate the importance of an event in which the S.M.A.R.T status of the physical device is Not Available. The default is 5.
Error Settings	
Raise event when physical device errors exceed threshold?	Select **Yes** to raise an event if the number of physical device errors exceeds the threshold you set. The default is Yes.
Threshold for device errors	Specify the maximum number of errors that can occur for a physical device before an event is raised. The default is 5.
Event severity when device errors exceed threshold	Set the severity level from 1 to 40 to indicate the importance of an event in which physical device errors exceed the threshold you set. The default is 15.
Data Collection	
Collect data for physical device status?	Set to **Yes** to collect data for charts and reports. If set to Yes, this Knowledge Script records the operational status of the device at each monitoring interval. The default is unselected.
Collect data for physical device errors?	Set to **Yes** to collect data for charts and reports. If set to Yes, this Knowledge Script records the number of errors of the device at each monitoring interval. The default is unselected.
Collect data for physical device S.M.A.R.T. status?	Set to **Yes** to collect data for charts and reports. If set to Yes, this Knowledge Script records the S.M.A.R.T. status of the device at each monitoring interval. The default is unselected.

MemoryModule

Use this Knowledge Script to monitor the status of memory modules on the system board. If a memory module fails or its status is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

If a memory module experiences frequent errors, locate and replace the defective memory module.

Resource Objects

Memory Module icon.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the memory module is operating properly • **50** if the memory module status is unknown • **0** if the memory module has failed The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...memory module failed**. The default is 5 (red event indicator). • **...status unknown**. The default is 25 (blue event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

NICError

Use this Knowledge Script to monitor network interface transmission errors. Both input and output errors are reported and evaluated against the thresholds you specify. If the number of network interface errors per minute exceeds the threshold, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

Network Interface Card (NIC) folder or individual NIC icons.

Default Schedule

The default interval for this Knowledge Script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the number of input and output errors per minute at each monitoring interval. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Maximum threshold for input errors per minute	Specify the maximum number of input errors that can occur per minute before an event is raised. The default is 2 errors per minute.
Maximum threshold for output errors per minute	Enter a threshold for the maximum number of output errors per minute. The default is 4 errors per minute.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...SNMP or ServerView service down**. The default is 9 (red event indicator). • **...input error threshold exceeded**. The default is 10 (red event indicator). • **...output error threshold exceeded**. The default is 10 (red event indicator).

NICFail

Use this Knowledge Script to monitor the status of the network interface. This Knowledge Script checks whether the network interface subsystem is down when the administrator has indicated it should be in the "up" state. If the network interface subsystem is down, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

Network Interface Card (NIC) folder or individual NIC icons.

Default Schedule

The default interval for this Knowledge Script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the operational status of the network interface subsystem at each monitoring interval. The default is n.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...network interface subsystem is down**. The default is 6 (red event indicator). • **...SNMP or ServerView service down**. The default is 9 (red event indicator).

OverallCondition

Use this Knowledge Script to monitor the overall condition of the discovered subsystems on the server such as, mass storage, system board, power supply, and environment. If a subsystem is not operating properly, this Knowledge Script raises an event.

Notes

You cannot customize the parameters to specify what subsystems need to be monitored by this Knowledge Script.

When this Knowledge Script raises an event, the event message does not indicate the subsystem having a problem. It displays a generic message that some of the subsystems are not working properly.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

If the overall condition of a device degrades, use the Siemens-related Knowledge Scripts to identify the source of the problem. To monitor Siemens ServerView services, see HealthCheck.

Resource Objects

Siemens Server.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data. If set to y, this Knowledge Script returns: • **100** if the overall condition is normal • **50** if the overall condition has degraded • **0** if the server encountered an error The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...device error or failed**. The default is 5 (red event indicator). • **...unknown subsystem status**. The default is 10 (red event indicator). • **...device degraded**. The default is 15 (yellow event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

PowerSupply

Use this Knowledge Script to monitor the status of one or more internal power supply units. If a power supply unit is not operational or its status is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

Power Supply folder or individual Power Supply icons.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: • **100** if the power supply is operating properly • **30** if the power supply status is unknown • **0** if the power supply has failed The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...power supply failed**. The default is 5 (red event indicator). • **...power supply status unknown**. The default is 25 (blue event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

SCSIPhysicalDevice

Use this Knowledge Script to monitor discovered SCSI physical devices such as, disk or CD-ROM devices. If a device fails, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

SCSI folder or individual SCSI icons.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns 100 if the SCSI device is operating properly or 0 if the SCSI device has failed. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for	Set the event severity level, from 1 to 40, to indicate the importance of: • **...SCSI physical device failure**. The default is 5 (red event indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

Temperature

Use this Knowledge Script to monitor the thermal environment and the status of the thermal sensors of the server. If a sensor is operating out of normal temperature range, or if the thermal status is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

Resource Objects

Temperature folder or individual Temperature icons.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the temperature (in degrees Celsius) at each monitoring interval. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...temperature abnormal or sensor failed**. The default is 15 (yellow event indicator). • **...temperature critical**. The default is 5 (red event indicator). • **...temperature status unknown**. The default is 25 (blue indicator). • **...SNMP or Siemens ServerView service down**. The default is 10 (red event indicator).

Voltage

Use this Knowledge Script to monitor the voltage level for a Siemens server. This Knowledge Script monitors the status of the voltage sensors on the system board. If a sensor detects that the voltage level has dropped below or exceeded the normal operating threshold, or the voltage level is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

The server system defines the voltage levels for normal operation internally.

Resource Objects

Voltage folder or individual Voltage icons.

Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the voltage level for each voltage sensor at each monitoring interval. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...voltage is too high or low**. The default is 5 (red event indicator). • **...voltage status unknown**. The default is 25 (blue indicator). • **...SNMP or ServerView service down**. The default is 10 (red event indicator).

Chapter 64
Snmp Knowledge Scripts

The Snmp category provides a set of Knowledge Scripts for monitoring SNMP-enabled devices. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Many Snmp Knowledge Scripts use the terms "ODE" or "OID":

- **ODE**: SNMP Object Description in its readable, named format. For example, "`system.sysDescr.0`" is the ODE for the numeric OID "`.1.3.6.1.2.1.1.0`".
- **OID**: SNMP Object Identifier in its numeric format. For example, "`.1.3.6.1.2.1.1.0`" is the OID for the SNMP attribute "`system.sysDescr.0`".

The Snmp category includes the following Knowledge Scripts:

Knowledge Script	What It Does
AddMIBs	Copies the specified list of MIB files to the AppManager agent host where you installed AppManager for SNMP. Reloads the MIB tree for the module so the new MIBs are recognized.
DeviceReboot	Monitors device uptime for an SNMP device and raises an event if the device has restarted since the last monitoring interval.
InterfaceState	Monitors the contents of the Interface MIB from an SNMP device and raises an event when an interface changes state.
RemoveMIBs	Removes the specified list of MIB files from the AppManager agent host where you installed AppManager for SNMP. Reloads the MIB tree for the module so the removed MIBs are no longer accessible.
SNMPTrap_Async	Checks for incoming SNMP traps forwarded from NetIQ SNMP Trap Receiver.
SyncGet	Attempts an SNMP `Get` or `GetNext` for the specified SNMP attributes. Thresholds can be checked, and mathematical conversions can be performed.
SyncGetTable	Retrieves a specified set of SNMP table columns, and reports results for each row retrieved. Thresholds can be checked, and mathematical conversions can be performed.
SyncPoll	Polls specified SNMP attributes at a prescribed time interval and number of polling attempts. Thresholds can be checked, and mathematical conversions can be performed.
SyncPollTable	Polls a specified set of SNMP table columns at a prescribed time interval and number of polling attempts, and reports summary results for each row polled. Thresholds can be checked, and mathematical conversions can be performed.
SyncSet	Attempts an `SNMP Set` for the specified SNMP attributes of the specified values.
Discovery_Snmp	Discovers SNMP devices at each IP address or hostname you specify.

Customizing Snmp Knowledge Scripts

There are several simple ways to customize Snmp Knowledge Scripts to enhance or add functionality. You can check out an existing script from the `\AppManager\bin\kp\SNMP` folder, perform customizations, and check in the modified script or rename the file to create a new Knowledge Script.

The following list describes how to customize existing Snmp scripts to take advantage of additional functions and features of AppManager for SNMP.

Enabling SNMP Traffic Tracing

You can enable SNMP Traffic Tracing for all Knowledge Scripts. Turning on Traffic Tracing prints the contents of all SNMP requests or SNMP responses to the `mctrace.log` file on the AppManager agent. This capability can be used as a debugging tool to determine what is actually being sent or received by AppManager for SNMP.

To enable SNMP Traffic Tracing for a specific Knowledge Script, locate the `Const gintSNMPSectionTraceOn` entry and change the value from "0" to "1". Check out the script, then locate and edit the following block of text accordingly:

```
'#
'# Constants for SNMP Traffic Tracing
'# Set gintSNMPSectionTraceOn to 1 to trace SNMP Traffic.
'# Output goes to the AppManager Agent's mctrace.log file.
'#
Const gintSNMPSectionTraceBit        = 1
Const gintSNMPSectionTraceOn        = 0
```

Changing default locations of community strings

You can change the default locations of community strings (as defined in the **Custom** tab of AppManager Security Manager) for all Knowledge Scripts except for AddMIBs and RemoveMIBs:

- `gstrSNMPSecurityLabels` lists the labels under which the Knowledge Script searches for community strings, in the order they are listed.
- `gstrSNMPDefaultDevice` specifies the **Sub-Label** used to supply the default community string if one has not been configured for a specific device address.

To edit these values, check out the desired Knowledge Script, then locate and edit the following block of text accordingly:

```
'#
'# String(s) to use for finding SNMP Community Strings
'#
Const gstrSNMPSecurityLabels      = "SNMP,NetworkDevice"
Const gstrSNMPDefaultDevice       = "Default"
```

Changing default list separator characters

Many Snmp Knowledge Script parameters are lists: devices, SNMP OIDs, and the like. The characters that serve as list separators can be changed. The defaults are blank and comma.

You can add additional list separator characters, but you cannot delete the comma character.

To edit these values, check out the desired script, then locate and edit the following block of text accordingly:

```
'#
'# Separators for KS Parameters
'#
Const gstrSNMPListSeparators      = " ,"
```

If you change `gstrSNMPListSeparators`, you must also add the `<Delim></Delim>` option to each script parameter's XML definition to specify the same separators defined by `gstrSNMPListSeparators`. If it is not changed in both places, the script will not work correctly.

For the SyncSet script, there is an additional constant: `gstrSNMPStringValueSeparators`. The default is "`,`" (comma). This specifies how SNMP values for this script are delimited. Because setting string values may include strings with spaces, only a comma is allowed as a separator. For example:

```
'#
'# Separators for KS Parameters
'#
Const gstrSNMPListSeparators         = " ,"
Const gstrSNMPStringValueSeparators  = ","
```

Default empty strings in the Discovery_Snmp script

For the Discovery_Snmp Knowledge Script, there are default strings defined to be used if any of the SNMP device details are empty strings. If `sysName.0` is an empty string, "`No Name`" is shown in the TreeView and the object details. All other object details will show "`No Value`" if they did not have a value. For example:

```
'#
'# String(s) to use for SNMP Devices with empty values in System MIB.
'#
Const gstrSNMPNoDeviceName        = "No Name"
Const gstrSNMPNoDeviceValue       = "No Value"
```

Changing default legend prefix and units for the DeviceReboot script

For the DeviceReboot Knowledge Script, the legend prefix and units in which device uptime is reported can be changed. For example, you could change it to Days by editing the text below and changing the divisor value to `86400`.

```
'#
'# Constants for Datastreams
'#
Const DEVICE_UPTIME_LEGEND       = "Device UpTime"
Const DEVICE_UPTIME_AC           = "Device UpTime (Hours)"
```

```
Const DEVICE_UPTIME_UNITS        = "Hours"
Const DEVICE_UPTIME_DIVISOR      = 3600
```

Changing default legend prefix for SyncGet and SyncGetTable scripts

For the SyncGet and SyncGetTable Knowledge Scripts, the legend prefix can be changed. Locate and edit the text below:

```
'#
'# Constant for SNMP Generic Scripts Legend Prefix
'#
Const gstrSNMPLegendPrefix        = "SNMP"
```

Note

If you rename a customized Knowledge Script, you cannot access Help using the **Help** button in the Knowledge Script Properties dialog box. Refer to the Help for the original script for assistance with parameter configuration.

AddMIBs

Use this Knowledge Script to install additional MIB files on an SNMP proxy agent computer. The specified files are copied to a default MIBs folder for the AppManager for SNMP module, and the module reloads the MIB tree so the new MIBs take effect.

This script copies files to and reloads both `AppManager/bin/AMSnmpMIBs` and `AppManager/bin/MIBs` directories. Both managed objects generate events for this script, and the short event messages include the name of the relevant managed object.

Run this script when no other SNMP scripts are active on the target proxy agent computer, because reloading the MIB tree can take place only when no SNMP sessions are active. If this script is unable to reload the MIB tree because of active SNMP sessions, an appropriate event can be raised. If no path or MIB files are supplied, by default this script creates an event containing a list of currently installed MIBs.

This script raises an event if the specified MIB files cannot be found, or an `ASN.1` compilation error occurs while reloading the MIB tree.

SNMP MIBs tend to be organized hierarchically. One MIB is often dependent on another, from which it imports more generic data definitions. Therefore, add a MIB only if all dependent MIBs are already present or are supplied in the same execution of this script.

Resource Object

SNMP Proxy Agent computer

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Full MIB file path	Specify the directory path where the MIB files to be installed are located. This script does not transfer the specified MIB files over the network. The directory path specified for the MIB files must already be locally accessible by the SNMP proxy agent computer.
List of MIB files	Supply a list of filenames for the MIBs you want to install. Do not include the directory path.
Reload MIB tree?	Set to **Yes** to reload the MIB tree after MIB files have been copied. A MIB tree reload is attempted only if all MIB files are installed successfully.
MIB reload timeout	Specify how long this script should wait to try and reload the MIB tree. This can only be performed if no other script has active SNMP sessions. The default is 10 seconds.
Event Notification	
Raise event if installation of MIBs succeeds?	Set to **Yes** to raise an event if all MIBs are installed successfully. The details of the event contain the list of installed MIB files.
Event severity when installation of MIBs succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB installation succeeds. The default is 25.

Parameter	How to Set It
Raise event if installation of MIBs fails?	Set to **Yes** to raise an event if any MIB files fail to install. This can occur if the path of MIB filenames specified is incorrect.
Event severity when installation of MIBs fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB installation fails. The default is 10.
Raise event if reloading of MIB tree succeeds?	Set to **Yes** to raise an event if all MIB files install successfully and the MIB tree is reloaded successfully. This can only occur if the *Reload MIB tree?* parameter is enabled.
Event severity when reloading of MIB tree succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB tree reloading is successful. The default is 25.
Raise event if reload MIB parser warnings received?	Set to **Yes** to raise an event if all MIB files install successfully and reloading the MIB tree reports `ASN.1` parsing errors. This can only occur if the *Reload MIB tree?* parameter is enabled. Details of the parsing errors are in the event.
Event severity when reload MIB parser warnings received	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MIB reload generates warnings. The default is 15.
Raise event if reloading of MIB tree fails?	Set to **Yes** to raise an event if all MIB files install successfully and reloading the MIB tree fails. This can occur if *Reload MIB tree?* is enabled and the *MIB reload timeout* expires.
Event severity when reloading of MIB tree fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB tree reload fails. The default is 10.

DeviceReboot

Use this Knowledge Script to monitor whether an SNMP device or its network management component has rebooted between job intervals. This script tracks the uptime value of the host (`hrSystemUptime.0`) or the network management component (`sysUpTime.0`) across job iterations to determine whether devices have rebooted. If the uptime value is less than the last iteration, the device has either rebooted or the uptime counter value has wrapped.

This script attempts to track `sysUpTime.0` on all SNMP devices where the script is run, regardless of whether any previous attempts have failed. If failures do occur, successful retrievals on other devices are not discarded.

This script generates data streams for each monitored SNMP device. The data value saved is the current number of hours the device has been up.

Resource Objects

SNMP Device objects

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
SNMP Parameters	
SNMP port number	Specify the UDP port number on the remote SNMP device to which you want to send SNMP requests. The default is 161.
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Collect data for device uptime?	Set to **Yes** to collect data for use in graphs and reports. If data collection is enabled, returns the device uptime in hours. The default is unchecked.
Monitor host uptime or uptime of the network management portion of the system?	Specify whether you want to monitor the uptime of the SNMP device or its network management component. The default is Host uptime.
Event Notification	
Raise event if device has rebooted?	Set to **Yes** to raise an event if a device reboot is detected. The details of the event contain the retrieved data.
Event severity when device has rebooted	Set the severity level, from 1 to 40, to indicate the importance of an event in which a device reboots. The default is 15.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise an event if the SNMP `Get` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout threshold is exceeded. The default is 15.

Description	How to Set It
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP Response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.
Raise event if device uptime baseline established?	Set to **Yes** to raise an event when initial data values are retrieved, setting the baseline for comparison on the next retrieval.
Event severity when device uptime baseline established	Set the severity level, from 1 to 40, to indicate the importance of an event in which baseline is established. The default is 25.
Raise event if the host uptime is not available?	Set to **Yes** to raise an event when the host uptime is not available. The default is Yes.
Event severity when the host uptime is not available.	Set the severity level, from 1 to 40, to indicate the importance of an event in which the host uptime is not available. The default is 15.

InterfaceState

Use this Knowledge Script to monitor the state of all interfaces in a device. This script tracks the values of `ifAdminStatus` and `ifOperStatus` for each interface across job iterations. If the operational status of an interface changes, an event is raised indicating the time the change occurred. This script also verifies whether `ifAdminStatus` and `ifOperStatus` are in sync.

The script attempts to track interface state on all SNMP devices on which the script is run, regardless of whether any previous attempts failed. If failures do occur, successful retrievals on other devices are not discarded.

This script collects separate data streams for each interface in a device. The data value saved is an integer representing the current operational state of each interface.

Resource Objects

One or more SNMP Device objects

Default Schedule

By default, this script runs every hour.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
SNMP Parameters	
List of interface indices	By default, all interfaces are monitored. However, supplying a list of SNMP interface indices can restrict monitoring to those specific interfaces. Indices must be a single integer value. For example, "`1 4 7`" monitors only interfaces with an SNMP interface index of 1, 4 and 7.
Maximum number of interfaces to monitor	Specify the maximum number of interfaces to monitor. The default is 100.
SNMP port number	Specify the UDP port number on the remote SNMP device to which you want to send SNMP requests. The default is 161.
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Collect data for interface state?	Set to **Yes** to collect data for use in graphs and reports. If enabled, returns a data stream for each interface in the device indicating its state. The default is unchecked.
Event Notification	
Raise event if interface state mismatch detected?	Set to **Yes** to raise an event if an interface has values for `ifAdminStatus` and `ifOperStatus` that are not the same. The details of the event contain the retrieved data.
Event severity when interface state mismatch detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Interface State Mismatch exists. The default is 10.

Parameter	How to Set It
Raise event if interface state is up?	Set to **Yes** to raise an event if an interface has transitioned to the Up state since the last Knowledge Script iteration. The details of the event contain the retrieved data.
Event severity when interface state is up	Set the severity level, from 1 to 40, to indicate the importance of an event in which the interface state is Up. The default is 25.
Raise event if interface state is down?	Set to **Yes** to raise an event if an interface has transitioned to the Down state since the last Knowledge Script iteration. The details of the event contain the retrieved data.
Event severity when interface state is down	Set the severity level, from 1 to 40, to indicate the importance of an event in which the interface state is Down. The default is 15.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout is exceeded. The default is 15.
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP Response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.
Raise event if interface state baseline established?	Set to **Yes** to raise an event when initial data values are retrieved, setting the baseline for comparison on the next retrieval.
Event severity when interface state baseline established	Set the severity level, from 1 to 40, to indicate the importance of an event in which baseline is established. The default severity level is 25.

RemoveMIBs

Use this Knowledge Script to remove one or more MIB files from an SNMP proxy agent computer. The specified files are deleted from the installation folder, which by default is *installationfolder*\AppManager\bin\AMSnmpMIBs.

Run this script when no other SNMP Knowledge Scripts are active on the target AppManager for SNMP installation because reloading the MIB tree can only be done when no SNMP sessions are active. If the RemoveMIBs Knowledge Script is unable to reload the MIB tree because of active SNMP sessions, the script can raise an appropriate event.

This script raises an event if the specified MIB files cannot be deleted, or an `ASN.1` compilation error occurs while reloading the MIB tree.

SNMP MIBs tend to be hierarchical. That is, one MIB is often dependent on another, from which it imports more generic data definitions. Therefore, delete a MIB only if it has no other dependent MIBs installed.

Resource Object

SNMP Proxy Agent computer

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
List of MIB files to uninstall	Supply a list of MIB filenames to be deleted.
Reload MIB tree?	Set to **Yes** to reload the MIB tree after MIB files have been deleted. A MIB tree reload is only be attempted if all MIB files are deleted successfully.
MIB reload timeout	Specify how long this script should wait to try and reload the MIB tree. This can only be performed if no other Knowledge Scripts have active SNMP sessions. The default is 10 seconds.
Event Notification	
Raise event if uninstallation of MIBs succeeds?	Set to **Yes** to raise an event if all MIBs are deleted successfully. The details of the event contain the list of installed MIB files.
Event severity when uninstallation of MIBs succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which MIB uninstallation succeeds. The default is 25.
Raise event if uninstallation of MIBs fails?	Set to **Yes** to raise an event if any MIB files fail to delete. This can occur if any specified MIB filenames correspond to files not currently installed.
Event severity when uninstallation of MIBs fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which MIB uninstallation fails. The default is 10.
Raise event if reloading of MIB tree succeeds?	Set to **Yes** to raise an event if all MIB files uninstall successfully and the MIB tree is reloaded successfully. This can only occur if the *Reload MIB tree?* parameter is set to Yes.

Parameter	How to Set It
Event severity when reloading of MIB tree succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which MIB tree reload succeeds. The default is 25.
Raise event if reload MIB parser warnings received?	Set to **Yes** to raise an event if all MIB files uninstall successfully and reloading the MIB tree reports `ASN.1` parsing errors. This can only occur if the *Reload MIB tree?* parameter is set to Yes. Details of the parsing errors are in the event.
Event severity when reload MIB parser warnings received	Set the severity level, from 1 to 40, to indicate the importance of an event in which MIB reload warnings are received. The default is 15.
Raise event if reloading of MIB tree fails?	Set to **Yes** to raise an event if all MIB files uninstall successfully but reloading the MIB tree fails. This can occur if the *Reload MIB tree?* parameter is set to Yes and the *MIB Reload timeout* expires.
Event severity when attempt to reload MIB tree fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which MIB tree reload fails. The default is 10.

SNMPTrap_Async

Use this Knowledge Script to check for SNMP traps forwarded from NetIQ SNMP Trap Receiver. This script raises an event when an SNMP trap is received and when Trap Receiver is unavailable or subsequently becomes available. In addition, this script generates data streams for Trap Receiver availability.

This script checks for SNMP traps in the MIB tree. You can add MIBs (management information bases) to the MIB tree. For more information, see the AddMIBs Knowledge Script.

In general, a trap receiver is an application that receives traps from SNMP agents. NetIQ SNMP Trap Receiver (Trap Receiver) receives SNMP traps, filters them, and then forwards the traps to AppManager.

Resource Object

SNMP_TrapReceiver

Default Schedule

By default, this script runs on an asynchronous schedule.

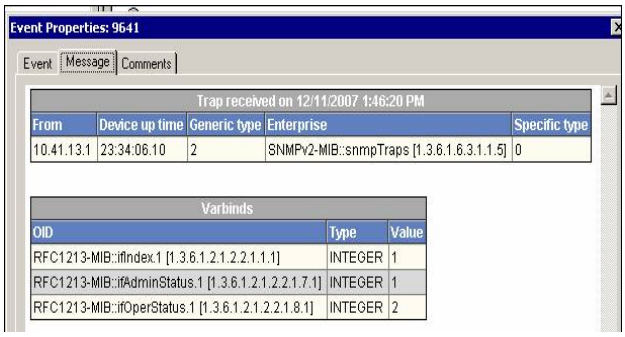
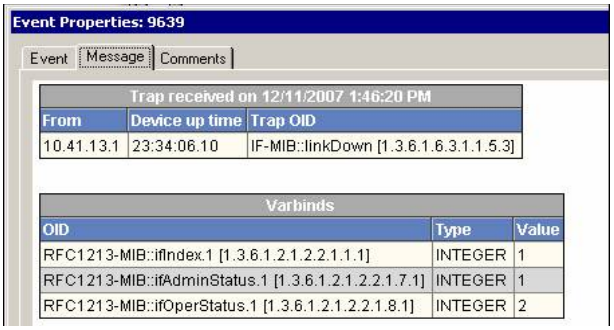
Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Trap Filters	
List of trap OIDs	Type the OIDs (object identifiers) of the traps you want to monitor. You can type one OID or a list of OIDs. Separate multiple OIDs with a comma, for example: `1.3.6.1.2.1.2.2.1.1.1,1.3.6.1.2.1.2.2.1.7.1`

Full path to file with list of trap OIDs	If you have many OIDs to monitor, provide the full path to a file that contains a list of the OIDs. Each OID in the file should be on a separate line, for example:
	`1.3.6.1.2.1.2.2.1.1.1`
	`1.3.6.1.2.1.2.2.1.7.1`
	Because the file must be accessible from the AppManager agent, the path must be a local directory on the agent computer or a UNC path.
	Important If you type a UNC path, then the `netiqmc` service must be running as a user that has access to the path.

Event Notification	
Raise trap events?	Set to **Yes** to raise an event when a trap message is received from Trap Receiver. The default is Yes.
Event severity when trap is received	Set the severity level, from 1 and 40, to indicate the importance of an event in which a trap is received. The default is 15.

Parameter	How to Set It
Format trap data according to SNMP version	Select the version of SNMP whose formatting should be used for trap event messages. The data provided by each format is the same; only the layout is different. An event message in SNMP v1 format looks like this:  An event message in SMMP v2 format looks like this: 
Raise Trap Receiver availability events?	Set to **Yes** to raise an event when Trap Receiver becomes unavailable and when Trap Receiver becomes available once again. The default is Yes.
Event severity when Trap Receiver is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes unavailable. The default is 5.
Event severity when Trap Receiver becomes available	Set the severity level, from 1 to 40, to indicate the importance of an event in which Trap Receiver becomes available after being unavailable. The default is 25.
Data Collection	
Collect data for Trap Receiver availability?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns a “1” if Trap Receiver is available and a “0” if Trap Receiver is unavailable. The default is unchecked.
Interval for collecting Trap Receiver availability data	Specify the frequency with which the script collects Trap Receiver availability data. The default is every 5 minutes.

SyncGet

Use this Knowledge Script to perform an SNMP `Get` or `GetNext` operation for one or more SNMP attributes from one or more SNMP enabled devices. This script raises an event if retrieved values exceed the threshold you set.

The script attempts to get the specified attributes on all supplied SNMP devices, regardless of whether any previous attempts failed. If failures do occur, successful gets on other devices are not discarded.

This script can independently collect separate data streams for each SNMP device/SNMP attribute pairing. Thus, the total number of data streams collected is the number of devices the script has been run on in the TreeView, multiplied by the number of SNMP attributes provided.

Note
Supply either all-numeric SNMP attributes or all-string SNMP attributes, because you must choose either a numeric check or string check. SNMP attributes that are octet strings, OIDs, or IP addresses are considered to be string attributes.

If one or more numerical conversions are selected, they are performed in the following order: Multiplication, Division, Delta and Percentage. If Delta and Division are both selected, integer division is performed and any remainder is discarded. If Delta is not selected, real-number division is performed.

Values reported in SNMP Success events show the results of multiplication and division conversions, but not delta and percentage conversions, as these are performed after the Success event has been raised. The final result of all conversions is shown in any threshold events, or in the data points if data is collected.

This script can be run at intervals to periodically poll SNMP attributes. However, if delta calculations are being performed on the retrieved values, the script interval should not be less than one minute, because the accuracy of delta calculations is time dependent and may not produce reliable results at shorter intervals. This is due to many factors including the accuracy of AppManager job scheduling and network traffic delay. The SyncPoll script should be used to accurately poll at intervals of less than one minute.

By default, this script retrieves `sysUpTime.0` from the device, converts the retrieved value to “Days”, and reports the retrieved value in a success event.

Resource Objects

One or more SNMP Device objects

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Get Parameters	
SNMP ODE/OIDs	Supply a list of SNMP Attribute ODEs and/or OIDs. Use ODEs only if the SNMP proxy agent computer has the corresponding MIB available. The default is `sysUpTime.0`.

Parameter	How to Set It
SNMP port number	Specify the UDP port number on the remote SNMP device to which you want to send SNMP requests. The default is 161.
SNMP retries	Specify the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Specify the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Perform GetNext instead of Get?	Set to **Yes** to perform an SNMP `GetNext` operation instead of a `Get`. The default is to perform a `Get` operation.
OID Value Check	
Collect data for OID value?	Set to **Yes** to collect data for use in graphs and reports. If enabled, returns a data stream for each SNMP device/SNMP attribute pair. The default is unchecked.
Calculated units	If this script is performing numeric conversions, a name for the resulting units calculated can be entered here. If nothing is supplied for this parameter, the default units are the name of the data type retrieved. The default is “Days”.
Calculate delta for numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and a delta should be calculated. The difference between the new value and the previous value is calculated. Normally this is used to monitor growth of SNMP counter values between iterations. The default is unchecked. Delta calculations are not normalized. Thus, it is usually necessary to perform a division conversion on delta calculations to convert to the desired time units. For example, if the growth of an SNMP counter is being tracked by doing a delta calculation at a script interval of one minute, it is necessary to divide by 60 to track the growth of the counter on a per-second basis. If set to **Yes**, **integer math** (not **floating point math**) is used; thus, any remainder is discarded. **Note** Do not enable this option if the script is running at intervals of less than one minute. The results may not be reliable.
Use multiplier for numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and should be multiplied by the value specified for the next parameter. The default is unchecked.
Multiplier value	If the *Use multiplier for numeric OID value?* parameter is enabled, the retrieved SNMP attributes are multiplied by this value before being reported. The default is 1.
Use divisor for numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and should be divided by the value specified for the next parameter. If you enabled the *Calculate delta for numeric OID value* parameter, integer division is performed and any remainder is discarded. Otherwise, values are converted to real numbers to perform the division and retain the precision of any remainder. The default is Yes.
Divisor value	If the *Use divisor for numeric OID value?* parameter is enabled, the retrieved SNMP attributes are divided by this value before being reported. The default is `8640000`.
Calculate percentage of numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and should be converted to a percentage of the maximum value supplied in the next parameter. Values are converted to real numbers to perform the percentage calculation and retain the precision of any remainder. Calculated values are restricted to a real number between 0% and 100%. The default is unchecked.

Parameter	How to Set It
Maximum value	If the *Calculate percentage of numeric OID value?* parameter is enabled, the retrieved SNMP attributes are converted to a percentage of the maximum value entered here. The default is 100.
Raise event when maximum threshold exceeded?	Set to **Yes** to specify that the retrieved values should be compared against the maximum threshold value supplied in the next parameter. If enabled, the check is performed after any mathematical conversions that may have been selected above. The default is unchecked.
Threshold -- Maximum OID value (post-calculation)	This parameter has no effect unless *Raise event when maximum threshold exceeded?* is enabled. For numeric attributes, specify the maximum threshold value. If this value is exceeded, an event is raised. The threshold value is restricted to whole integer values. The default is 1000.
Raise event when minimum threshold not met?	Set to **Yes** to specify that the retrieved values should be compared against the minimum threshold value supplied in the next parameter. If enabled, the check is performed after any mathematical conversions that may have been selected above. The default is unchecked.
Threshold -- Minimum OID value (post-calculation)	This parameter has no effect unless *Raise event if threshold not met?* is enabled. For numeric attributes, specify the minimum threshold value. If this threshold is not met, an event is raised. The threshold value is restricted to whole integer values. The default is 100.
Raise event when returned value equals “Numeric value”?	Set to **Yes** to raise an event when the retrieved numeric values equal the value supplied in the *Numeric value* parameter. If enabled, the check is performed after any mathematical conversions that may have been selected above.
Check for “not equal” instead of “equals”?	Use this parameter to change the function of the previous parameter. To raise an event when the retrieved numeric values do not equal the value supplied in the *Numeric value* parameter, set to **Yes** and ensure that *Raise event when returned value equals “Numeric value”?* is also set to **Yes**.
Numeric value	Use this parameter only if *Raise event when returned value equals “Numeric value”?* is enabled. An event is raised if the retrieved SNMP values equal the value you enter here. If *Check for “not equal” instead of “equals”?* is also enabled, an event is raised if the retrieved SNMP values are not equal to the value you enter here. This threshold is restricted to whole integer values. The default is 0.
Raise event when returned string equals “String value”?	Set to **Yes** to raise an event when the retrieved values equal the value supplied in the *String value* parameter. Use this parameter to retrieve SNMP attributes that are strings, octet strings, OIDs, or IP addresses.
Check for “not equal” instead of “equals”?	Use this parameter to change the function of the previous parameter. To raise an event when the retrieved values do not equal the value supplied in the *String value* parameter, set to **Yes** and ensure *Raise event when returned string equals “String value”?* is also set to **Yes**.
Do case-insensitive comparison?	If *Raise event when returned string not equal to value?* is enabled, set to **Yes** to specify that the retrieved values should be compared without regard to character case.
String value	Use this parameter only If *Raise event when returned string equals “String value”?* is enabled. An event is raised if the retrieved string equals the value you enter here. If *Check for “not equal” instead of “equals”?* is also enabled, an event is raised if the retrieved string does not equal the value you enter here. The default is “`String Value`”.

Parameter	How to Set It
Event severity when OID value violates check	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is crossed or an equality/inequality check fails. The default is 5.
Event Notification	
Raise event if SNMP operation succeeds?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` operation is successful. The details of the event contain the retrieved data.
Event severity when SNMP operation succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP operation succeeds. The default is 25.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout period is exceeded. The default is 15.
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP Response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.
Raise event if delta baseline established?	This event can be raised only if the *Calculate delta for numeric OID value?* parameter is enabled. Set to **Yes** to raise an event when the initial value is retrieved, setting the baseline for a difference calculation on the next job iteration.
Event severity when delta baseline established	Set the severity level, from 1 to 40, to indicate the importance of an event in which a delta baseline is established. The default is 25.

SyncGetTable

Use this Knowledge Script to perform an SNMP table walk along specified columns of an SNMP table. This script raises an event if retrieved values exceed the threshold you set.

Note
Because this script walks an SNMP table, do not supply an index value on the ODE/OIDs. Supplying just the attribute name (for example, "ifDescr") is normally sufficient. If only a portion of the table is to be walked, a parameter is available to specify the subset of table indices to walk.

The table walk is performed with iterative `GetNext` operations. As soon as any of the attributes walk beyond the end of the table, or the table indices become out of sync, the table walk terminates. If a table is fully populated, all attributes or table columns walk beyond the end of the table on the same `GetNext` operation. However, if the table has missing values, the table indices become out of sync as soon as a missing value is reached. A table walk is terminated when the first missing value is detected.

This script attempts to walk the specified attributes on all SNMP devices on which this script has been run, regardless of whether any previous attempts failed. If failures do occur, successful walks on other devices are not discarded.

This script individually collects separate data streams for each SNMP device/data OID pairing. Thus, the total number of data streams collected is the number of devices the Knowledge Script is run on multiplied by the number of data OIDs and the number of rows in the table on each device.

Note
Supply either all-numeric SNMP attributes or all-string SNMP attributes because you must choose either a numeric check or string check. SNMP attributes that are octet strings, OIDs, or IP addresses are considered to be string attributes.

If one or more numerical conversions are selected, they are performed in the following order: Multiplication, Division, Delta and Percentage. If Delta and Division are both enabled, integer division is performed, and any remainder is discarded. If Delta is not enabled, real-number division is performed.

Values reported in SNMP Success events show the results of multiplication and division conversions, but not delta or percentage conversions, as these are performed after the Success event has been raised. The final result of all conversions is shown in any threshold-crossing events or reflected in the data streams if data is collected.

This script can be run at intervals to periodically poll SNMP tables. However, if delta calculations are being performed on the retrieved values, the script interval should not be less than one minute, because the accuracy of delta calculations is time dependent and may not produce reliable results at shorter intervals. This unreliability is due to many factors including the accuracy of AppManager job scheduling and network traffic delay. The SyncPollTable Knowledge Script should be used to accurately poll at intervals of less than one minute.

By default, this script retrieves the operational status for all interfaces on a device.

Resource Objects

SNMP Device objects

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Get Table Parameters	
Descriptive ODE/OIDs	Supply a list of SNMP attribute ODEs and/or OIDs. These are descriptive attributes only, which are reported in event and data details for reference purposes. No processing is performed on the retrieved values. The attributes chosen should uniquely identify the retrieved row of an SNMP Table. The default is "`ifIndex, ifDescr`", which identifies the row number and name of a communications interface in the device.
Data ODE/OIDs	Supply a list of SNMP attribute ODEs and/or OIDs. ODEs can only be used if the SNMP proxy agent computer has the corresponding MIB available. The default is `ifOperStatus`.
Optional table indices	By default, the entire SNMP table is walked. However, supplying a list of the table indices to be walked can restrict the walk. Indices can be a single integer value, or multiple integer values separated by dots; just like a numeric OID value but without a leading dot. For example, "1.10.42.1.47" is a valid table index.
Maximum number of table rows to get	Specify the maximum number of table rows to be retrieved. The default is 100.
SNMP port number	Specify the UDP port number on the remote SNMP device to which you want to send SNMP requests. The default is 161.
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
OID value check	
Collect data for OID value?	Set to **Yes** to collect data for graphs and reports. The data is stored in the AppManager repository. When enabled, returns a data stream for each SNMP device/SNMP attribute pair. The default is unchecked.
Calculated units	If this script is performing numeric conversions, a name for the resulting units calculated can be entered here. If nothing is supplied for this parameter, the default units are the name of the data type retrieved. The default is blank.

Parameter	How to Set It
Calculate delta for numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and the difference between the new value and the previous value should be calculated. Normally this is used to monitor growth of SNMP counter values between iterations. The default is unchecked. Delta calculations are not normalized. Thus, it is usually necessary to perform a division conversion on delta calculations to convert to the desired time units. For example, if the growth of an SNMP counter is being tracked by doing a delta calculation at a script interval of one minute, it is necessary to divide by 60 to track the growth of the counter on a per second basis. If set to **Yes**, **integer math** (not **floating point math**) is used, thus any remainder is discarded. **Note** Do not enable this option if the script is running at intervals of less than one minute. The results may not be reliable.
Use multiplier for numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and should be multiplied by the value in the next parameter. By default, multiplication is not performed on retrieved values.
Multiplier value	If the *Use multiplier for numeric OID value?* parameter is enabled, the retrieved SNMP attributes are multiplied by this value before being reported. The default is 1.
Use divisor for numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and should be divided by the value in the next parameter. If the *Calculate delta for numeric OID value* parameter has also been enabled, integer division is performed and any remainder is discarded. Otherwise, values are converted to real numbers to perform the division and retain the precision of any remainder. The default is unchecked.
Divisor value	If the *Use divisor for numeric OID value?* parameter is enabled, the retrieved SNMP attributes are divided by this value before being reported. The default is 1.
Calculate percentage of numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and should be converted to a percentage of the *Maximum value*. Values are converted to real numbers to perform the percentage calculation and retain the precision of any remainder. Calculated values are restricted to a real number between 0% and 100%. The default is unchecked.
Maximum value	If the *Percentage of numeric OID value?* parameter is enabled, the retrieved SNMP attributes are converted to a percentage of the maximum value entered here. The default is 100.
Raise event when maximum threshold exceeded?	Set to **Yes** to specify that the retrieved values should be compared against the maximum threshold value supplied in the next parameter. If enabled, the check is performed after any mathematical conversions that may have been selected above. The default is unchecked.
Threshold -- Maximum OID value (post-calculation)	This parameter has no effect unless *Raise event if threshold exceeded?* is enabled. For numeric attributes, specify the maximum threshold value. If this value is exceeded, an event is raised. The threshold value is restricted to whole integer values. The default is 1000.
Raise event when minimum threshold not met?	If *Raise event if threshold not met?* is enabled, set to **Yes** to specify that the retrieved values should be compared against the minimum threshold value supplied in the next parameter. If enabled, the check is performed after any mathematical conversions that may have been selected above. The default is unchecked.

Parameter	How to Set It
Threshold -- Minimum OID value (post-calculation)	If the *Raise event if threshold not met?* parameter is enabled, specify a minimum value for numeric attributes after any calculations have been performed. If this threshold is not met, an event is raised. The threshold value is restricted to whole integer values. The default is 100.
Raise event when returned value equals "Numeric value"?	Set to **Yes** to raise an event when the retrieved numeric values equal the value supplied in the *Numeric value* parameter. If enabled, the check is performed after any mathematical conversions that may have been selected above.
Check for "not equal" instead of "equals"?	Use this parameter to change the function of the previous parameter. To raise an event when the retrieved numeric values do not equal the value supplied in the *Numeric value* parameter, set to **Yes** and ensure that *Raise event when returned value equals "Numeric value"?* is also set to **Yes**.
Numeric value	Use this parameter only if *Raise event when returned value equals "Numeric value"?* is enabled. An event is raised if the retrieved SNMP values equal the value you enter here. If *Check for "not equal" instead of "equals"?* is also enabled, an event is raised if the retrieved SNMP values do not equal the value you enter here. This threshold is restricted to whole integer values. The default is 0.
Raise event when returned string equals "String value"?	Set to **Yes** to raise an event when the retrieved values equal the value supplied in the *String value* parameter. Use this parameter to retrieve SNMP attributes that are strings, octet strings, OIDs, or IP addresses.
Check for "not equal" instead of "equals"?	Use this parameter to change the function of the previous parameter. To raise an event when the retrieved values do not equal the value supplied in the *String value* parameter, set to **Yes** and ensure *Raise event when returned string equals "String value"?* is also set to **Yes**.
Do case-insensitive comparison?	If *Raise event when returned string not equal to value?* is enabled, set to **Yes** to specify that the retrieved values should be compared without regard to character case.
String value	Use this parameter only If *Raise event when returned string equals "String value"?* is enabled. An event is raised if the retrieved string equals the value you enter here. If *Check for "not equal" instead of "equals"?* is also enabled, an event is raised if the retrieved string does not equal the value you enter here. The default is "`String Value`".
Event severity when OID value violates check	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is crossed or an equality/inequality check fails. The default is 5.
Event Notification	
Raise event if SNMP operation succeeds?	Set to **Yes** to raise events if the SNMP `Get` or `GetNext` operation is successful. The details of the event contain the retrieved data.
Event severity when SNMP operation succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP operation succeeds. The default is 25.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise events if the SNMP `Get` or `GetNext` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout period is exceeded. The default is 15.
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP Response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.

Parameter	How to Set It
Raise event if delta baseline established?	If *Calculate delta for numeric OID value?* has been enabled, set to **Yes** to raise an event when the initial value is retrieved, setting the baseline for a difference calculation on the next retrieval.
Event severity when delta baseline established?	Set the severity level, from 1 to 40, to indicate the importance of an event in which a delta baseline is established. The default is 25.

SyncPoll

Use this Knowledge Script to poll SNMP attributes on a Device at short time intervals during each Knowledge Script iteration. Only numeric SNMP attributes may be polled. For each set of polled values, this script computes a minimum, maximum, average and standard deviation. This script raises an event if computed values exceed the threshold you set.

When this script is run on multiple devices, they are polled successively, and not simultaneously. To poll devices simultaneously, a different job must be created for each device.

Note
The number of Polling attempts multiplied by the Polling interval and then multiplied by the number of devices on which the Knowledge Script is run must not exceed the time interval between Knowledge Script iterations. Attempting to do so causes the script to abort, as the polling would not be able to complete before the next iteration is due to execute.

This script continues polling the SNMP device regardless of whether any previous attempts failed. At least two polling attempts must succeed for any meaningful data to be calculated.

This script individually collects separate data streams for each SNMP attribute. By default, this script calculates the percent bandwidth utilization for the first interface listed in the `ifTable` for the SNMP device, assuming the speed of this interface is standard Ethernet of 100 Megabits per second. If the speed of this interface is different, the values returned by the default settings are not valid.

If one or more numerical conversions are selected, they are performed in the following order: Delta, Multiplication, Division and Percentage.

When polling the growth of SNMP counter values using the Delta option, all values are normalized on a per second basis, regardless of the length of the polling interval. For example, this script can be used to calculate the Kilobytes per second flowing through an interface by polling `ifInOctets` and `ifOutOctets` and dividing the returned values by 1024. The values reported are Kilobytes per second regardless of the length of the polling interval.

Resource Objects

SNMP Device objects

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Polling Parameters	
SNMP ODE/OIDs	Supply a list of SNMP attribute ODEs and/or OIDs. ODEs can only be used if the SNMP proxy agent computer has the corresponding MIB available. The default is: `"ifInOctets.1, ifOutOctets.1"`.
Polling interval	Specify the time interval between polling attempts during each Knowledge Script iteration. The default is 5 seconds.

Parameter	How to Set It
Polling attempts	Specify the number of polling attempts to perform during each Knowledge Script iteration. The default is 12. Combined with the default interval of 5 seconds, the script by default polls the SNMP device for 1 minute. The minimum value is 2.
SNMP port number	Specify the UDP port number on the remote SNMP device to which you want to send SNMP requests. The default is 161.
SNMP timeout	Specify the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Polled Values Check	
Collect data for polled values?	Set to **Yes** to collect data for use in graphs and reports. The data is stored in the AppManager repository. If enabled, returns a data stream for each SNMP device/SNMP attribute pair. The default is unchecked.
Polling calculation type	For each set of polled values, the Average, Minimum, Maximum and Standard Deviation are calculated. Use this parameter to select which calculated value serves as the data point.
Calculated units	Specify a name to identify the units being polled and calculated by this script. The default is “Percent”.
Calculate delta for polled value?	Set to **Yes** to specify that the retrieved values should be considered a delta from the value retrieved by the previous polling attempt. The difference between the new value and the previous value is calculated. Normally this is used to monitor growth of SNMP counter values between polling attempts. By default, a delta calculation is performed. When set to **Yes**, **integer math** (not **floating point math**) is used; thus, any remainder is discarded. **Note** When this parameter is enabled, the script reports one less polling attempt than was specified for *Polling attempts* because the first polling attempt is used to set a baseline for the delta calculations to follow.
Use multiplier for polled value?	Set to **Yes** to specify that the retrieved values are numeric and should be multiplied by the value in the next parameter. The default is unchecked.
Multiplier value	If the *Use multiplier for numeric OID value?* parameter is enabled, the retrieved SNMP attributes are multiplied by this value before being reported. The default is 1.
Use divisor for polled value?	Set to **Yes** to specify that the retrieved values should be divided by the value in the next parameter. Values are converted to real numbers to perform the division and retain the precision of any remainder. The default is unchecked.
Divisor value	If the *Use divisor for numeric OID value?* parameter is enabled, the retrieved SNMP attributes are divided by this value before being reported. The default is 1.
Calculate percentage of polled value?	Set to **Yes** to specify that the retrieved values should be converted to a percentage of the maximum value supplied in the next parameter. Values are converted to real numbers to perform the percentage calculation and retain the precision of any remainder. Calculated values are restricted to a real number between 0% and 100%. The default is Yes.
Maximum value	If the *Percentage of numeric OID value?* parameter is enabled, the retrieved SNMP attributes are converted to a percentage of the maximum value entered here. The default is 12500000 bytes (or 100 Megabits) per second.

Parameter	How to Set It
Raise event when maximum threshold exceeded?	Set to **Yes** to specify that the retrieved values should be compared against the maximum threshold value supplied in the next parameter. If enabled, the check is performed after any mathematical conversions that may have been selected above. The default is unchecked.
Threshold -- Maximum OID value (post-calculation)	This parameter has no effect unless *Raise event when maximum threshold exceeded?* is enabled. For numeric attributes, specify the maximum threshold value. If this value is exceeded by a retrieved value after any selected calculations have been performed, an event is raised. Polling threshold values are real numbers. The default is 90.
Raise event when minimum threshold not met?	Set to **Yes** to specify that the retrieved values should be compared against the minimum threshold value supplied in the next parameter.If enabled, the threshold check is done after any mathematical conversions that may have been selected above. The default is unchecked.
Threshold -- Minimum OID value (post-calculation)	This parameter has no effect unless *Raise event when minimum threshold not met?* is enabled. Specify a minimum threshold value. If the retrieved value fails to meet the threshold value after any calculations have been performed, an event is raised. Polling threshold values are real numbers. The default is 0.
Event severity when polled value violates check	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is crossed or an equality/inequality check fails. The default is 5.
Event Notification	
Raise event if SNMP operation succeeds?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` operation is successful. The details of the event contain the retrieved data.
Event severity when SNMP operation succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which an SNMP operation succeeds. The default is 25.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout period is exceeded. The default is 15.
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.

SyncPollTable

Use this Knowledge Script to perform an SNMP table walk along specified columns of an SNMP table. The retrieved table on the device is then polled at short time intervals at every script iteration. Only numeric attributes are polled. For each table row that is polled, this script computes a minimum, maximum, average and standard deviation. This script raised an event if the computed values exceed the threshold you set.

Note
Because this script walks an SNMP table, it is normally not necessary to supply an index value on the ODE/OIDs. Supplying just the attribute name (for example, "ifDescr") is normally sufficient. If only a portion of the table is to be walked, a parameter is available to specify the subset of table indices to walk.

The table walk is performed with iterative `GetNext` operations. As soon as any attribute walks beyond the end of the table, or the table indices become out of sync, the table walk terminates. If a table is fully populated, all attributes (or table columns) walk beyond the end of the table on the same `GetNext` operation. However, if the table has missing values, the table indices become out of sync as soon as a missing value is reached. A table walk is terminated when the first missing value is detected.

When this script is run on multiple devices, they are polled successively, not simultaneously. To poll devices simultaneously, create a different job for each device.

Note
The number of Polling attempts multiplied by the Polling interval and then multiplied by the number of devices on which the script is run must not exceed the time interval between script iterations. If this value does exceed the interval, the script job aborts because the polling would not be able to complete before the next Knowledge Script job is due to execute.

The script continues polling, regardless of whether any previous attempts failed. At least two polling attempts must succeed in order to report meaningful data.

This script collects separate data streams for each SNMP table row. Thus, the number of data streams is the number of SNMP data OIDs, multiplied by the number of rows in the table, and multiplied by the number of devices on which the script is run. By default, this script polls how many Kilobytes per second are flowing through each interface listed in the `ifTable` for the SNMP device.

If one or more numerical conversions are selected, they are performed in the following order: Delta, Multiplication, Division and Percentage. When polling growth of SNMP counter values using the Delta option, all values are normalized on a per second basis, regardless of the length of the polling interval. For example, as stated above by default this script calculates the Kilobytes per second flowing through all interfaces in the device. The values reported are Kilobytes per second regardless of the length of the polling interval.

Resource Object

Host System Folder running an AppManager agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Polling Table Parameters	
Descriptive ODE/OIDs	Supply a list of SNMP Attribute ODEs and/or OIDs. These are descriptive attributes only which are reported in event and data details for reference purposes, and no processing is done on the retrieved values. The attributes chosen should uniquely identify the retrieved row of an SNMP table. The default is "`ifIndex, ifDescr`", which identifies the row number and name of a communications interface in the device.
Data ODE/OIDs	Supply a list of SNMP Attribute ODEs and/or OIDs. ODEs can only be used if the AppManager for SNMP module on the proxy agent computer has the corresponding MIB available. The default is "`ifInOctets,IfOutOctets`".
Optional table indices	By default, the entire SNMP table is walked. However, supplying a list of the table indices to be walked can restrict the walk. Indices can be a single integer value, or multiple integer values separated by dots; just like a numeric OID value but without a leading dot. For example, "1.10.42.1.47" is a valid table index.
Maximum number of table rows to poll	Specify the maximum number of table rows to be polled. The default is 100.
Polling interval	Specify the time interval between polling attempts during each Knowledge Script iteration. The default is 5 seconds.
Polling attempts	Specify the number of polling attempts to perform during each Knowledge Script iteration. The default is 12. Combined with the default interval of 5 seconds, the script by default polls the SNMP device for 1 minute. The minimum value is 2.
SNMP port number	Specify the UDP port number on the remote SNMP device to which you want to send SNMP requests. The default is 161.
SNMP timeout	Specify the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Polled Values Check	
Collect data for polled values?	Set to **Yes** to collect data for use in graphs and reports. The data is stored in the AppManager repository. When enabled, returns a data stream for each SNMP device/SNMP attribute pair. The default is unchecked.
Polling calculation type	For each set of polled values, the Average, Minimum, Maximum and Standard Deviation are calculated. Use this parameter to select which calculated value serves as the data point for the retrieved values.
Calculated units	Specify a name to identify the units being polled and calculated by this script. The default is "Kbytes/Sec".
Calculate delta for polled value?	Set to **Yes** to specify that the retrieved values should be considered a delta from the value retrieved by the previous polling attempt. The difference between the new value and the previous value is calculated. Normally this is used to monitor growth of SNMP counter values between polling attempts. The default is Yes. When set to **Yes**, **integer math** (not **floating point math**) is used, thus any remainder is discarded. **Note** When you enable this parameter, this script reports one less polling attempt than was specified for *Polling attempts*, because the first polling attempt is used to set a baseline for the delta calculations to follow.
Use multiplier for polled value?	Set to **Yes** to specify that the retrieved values are numeric and should be multiplied by the value in the next parameter. The default is unchecked.

Parameter	How to Set It
Multiplier value	If *Use multiplier for numeric OID value?* is enabled, the retrieved SNMP attributes are multiplied by this value before being reported. The default is 1.
Use divisor for polled value?	Set to **Yes** to specify that the retrieved values are numeric and should be divided by the value in the next parameter. Values are converted to real numbers to perform the division and retain the precision of any remainder. The default is unchecked.
Divisor value	If *Use divisor for numeric OID value?* is enabled, the retrieved SNMP attributes are divided by this value before being reported. The default is 1.
Calculate percentage of polled value?	Set to **Yes** to specify that the retrieved values are numeric and should be converted to a percentage of the maximum value supplied in the next parameter. Values are converted to real numbers to perform the percentage calculation and retain the precision of any remainder. Calculated values are restricted to a real number between 0% and 100%. The default is unchecked.
Maximum value	If *Calculate percentage of numeric OID value?* is enabled, the retrieved SNMP attributes are converted to a percentage of the maximum value entered here. The default is 100.
Raise event when maximum threshold exceeded?	Set to **Yes** to specify that the retrieved values should be compared against the maximum threshold value supplied in the next parameter. If enabled, the check is performed after any mathematical conversions that may have been selected above. The default is unchecked.
Threshold -- Maximum OID value (post-calculation)	If *Raise event when maximum threshold exceeded?* is selected, specify a maximum threshold value. If a retrieved value exceeds the threshold, an event is raised. Polling threshold values are real numbers. The default is 1000.
Raise event when minimum threshold not met?	Set to **Yes** to specify that the retrieved values should be compared against the minimum threshold value supplied in the next parameter. If enabled, the check is performed after any mathematical conversions that may have been selected above. The default is unchecked.
Threshold -- Minimum OID value (post-calculation)	If *Raise event when minimum threshold not met?* is enabled, specify a minimum threshold value. If a retrieved value fails to meet this threshold, an event is raised. Polling threshold values are real numbers. The default is 100.
Event severity when polled value violates check	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is crossed or an equality/inequality check fails. The default is 5.
Event Notification	
Raise event if SNMP operation succeeds?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` is successful. The details of the event contain the retrieved data.
Event severity when SNMP operation succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which an SNMP operation is successful. The default is 25.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout interval is exceeded. The default is 15.
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP Response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.

SyncSet

Use this Knowledge Script to set one or more SNMP attributes on one or more SNMP-enabled devices to the specified values. The values can be of different types. However, so that the value types can be determined, the SNMP proxy agent computer that executes the script must have the MIB available for the specified attributes even if numeric OIDs are supplied. If the MIB for the specified attributes is not available, an SNMP `Failure` event is raised. Although requiring the MIB to be installed is a restriction, it does allow the flexibility to easily set multiple SNMP attributes of different types from a single script.

This script attempts to set the specified attributes on all supplied SNMP devices, regardless of whether any or all of the attempts fail. If failures do occur, successful sets on other devices cannot be reversed or backed out.

Collected data for this script is a Boolean value that specifies whether the SNMP `Set` operation failed or succeeded.

Resource Objects

SNMP Device objects

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
SNMP ODE/OIDs	Supply a list of ODEs and/or OIDs. The default is "`sysContact.0`".
SNMP values (comma-separated)	Supply a comma-separated list of SNMP attribute values. As some SNMP values could be text strings, commas must be used as separators rather than spaces. The list must contain the same number of items as the *SNMP ODE/OIDs* parameter, and should be in the order corresponding to their respective attribute. The default is "Your System Administrator".
SNMP port number	Specify the UDP port number on the remote SNMP device to which you want to send SNMP requests. The default is 161.
SNMP retries	Specify the number of retries to attempt if a timeout occurs on an SNMP request. The default is 0 retries.
SNMP timeout	Specify the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Set success	
Collect data for Set success?	Set to **Yes** to collect data for use in graphs and reports. The data is stored in the AppManager repository. When enabled, returns a data stream containing a Boolean value representing whether the `Set` request succeeded or failed.
Raise event if Set success not equal to threshold?	Set to **Yes** to raise an event if the result of the `Set` request is not equal to the threshold. The default is Yes.

Parameter	How to Set It
Threshold – Set success	Set this value to one of the following: • 1 -- the `Set` request succeeds • 0 -- the `Set` request does not succeed. The default is 1 (success).
Event severity when Set success not equal to threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which Set success is not equal to the threshold you set. The default is 15.
Event Notification	
Raise event if SNMP operation succeeds?	Set to **Yes** to raise an event if the SNMP `Set` operation is successful. The details of the event contain the list of attributes you set.
Event severity when SNMP operation succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP `Set` operation succeeds. The default is 25.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise an event if the SNMP `Set` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout interval is exceeded. The default is 15.
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP Response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.

Discovery_Snmp

Use this Knowledge Script to discover SNMP-enabled devices running on a network. The AppManager agent on which AppManager for SNMP is installed acts as a proxy for discovering SNMP devices. This AppManager agent is referred to as the SNMP proxy agent computer.

In a successful discovery, the following details are discovered:

Object	Discovered Details
SNMP Proxy object	Agent Address – The hostname or IP address of the SNMP proxy agent computer.
SNMP Device object	• Device Address — The hostname or IP address under which the device was discovered. • SNMP Version – The SNMP version being used by the SNMP device. • System Name – The value of the SNMP attribute `sysName.0`. • Vendor – The name of the vendor that manufactured the device. • OID – System OID from `sysObjectID.0` that uniquely identifies the type of device. • Services – The network services supported by the device, as specified by `sysServices.0`. • Contact – The value of `sysContact.0`. • Location – The value of `sysLocation.0`.

Devices can only be discovered by providing a device list of hostnames, IP addresses, or IP address ranges for the corresponding Discovery Knowledge Script parameters. There is no automatic discovery capability. The Discovery_Snmp script iteratively attempts to contact and retrieve the System MIB from each supplied hostname or IP address.

Because many SNMP devices (typically routers) have multiple IP addresses, some devices may be discovered multiple times. In these cases, the Discovery script automatically detects and removes the duplicates from the list of discovered devices. Any duplicates are shown in the AppManager TreeView pane under the IP address or hostname under which they were first discovered.

During discovery, various errors may occur with the supplied list of SNMP devices. Most commonly, these will be SNMP timeouts from devices failing to respond because they are down, because they are not running an SNMP agent, or because the community string supplied for the device is incorrect. Other common errors can be due to bad hostnames or SNMP Response errors.

Discovery can take anywhere from a few seconds to several minutes or hours. The time taken largely depends on how many SNMP timeouts occur. For example, if this script is configured with an *SNMP timeout* value of 5 seconds and 3 *SNMP retries*, it takes 20 seconds to determine that the device is not responding.

The time taken for discovery to finish can be controlled by limiting the use of IP address ranges, which are likely to contain many addresses that are not used or that do not correspond to SNMP devices, and to keep the SNMP timeout/retry values as small as is practical for the local network environment.

Prerequisite

Before using this script, configure AppManager Security Manager with the community string and version information for each device you want to discover.

Resource Objects

NT_MachineFolder

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Discovery Parameters	
List of SNMP devices	Supply a list of SNMP device hostnames or IP addresses for the devices you want to monitor. An attempt is made to discover each device listed. The default is `localhost`.
Address ranges of SNMP devices	Instead of listing each IP address individually in *List of SNMP devices*, you can provide a list of IP address ranges. Each range must be in the format "`A.B.C.D-W.X.Y.Z`". For example, enter "`10.1.1.0-10.1.1.254`". Each address range may be no longer than 255 addresses, although they can span subnets. For example, "`10.1.1.250-10.1.2.30`" spans a subnet.
Full path to file with list of SNMP devices	Instead of listing each IP address or range of addresses, you can supply the full path to a file containing a list of individual IP addresses or hostnames. The file path supplied must be accessible from the SNMP proxy agent computer, not the AppManager Operator Console or repository computer. Device names can be separated by commas, blank characters or new lines.
Maximum number of devices to discover	Specify the maximum number of devices to be discovered. Discovery stops when this limit is reached, even if not all IP addresses and hostnames have been attempted. The default and maximum allowed value is 50.
SNMP port number	Specify the UDP port number on the remote SNMP device to which you want to send SNMP requests. The default is 161.
SNMP retries	Specify the number of retries to attempt if a timeout occurs on an SNMP request. The default is 1 retry.
SNMP timeout	Specify the number of seconds to wait for a response before timing out an SNMP request. The default is 3 seconds.
Trap Receiver Discovery	
Discover Trap Receiver?	Set to **Yes** to discover NetIQ SNMP Trap Receiver. The default is Yes.
Trap Receiver IP address	Specify the IP address of the computer on which Trap Receiver is installed. The default is `localhost`.
Trap Receiver TCP port	Specify the TCP port number through which Trap Receiver will communicate with AppManager. The default is port 2735.
Event Notification	
Raise event if discovery succeeds?	Set to **Yes** to raise an event if discovery is completely successful. The details of the event contain the list of discovered devices.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25. Discovery is successful if all devices in the device list are discovered and no errors occur. The event message indicates any duplicate IP addresses or hostnames. Duplicates are not considered to be an error.

Parameter	How to Set It
Raise event if discovery partially succeeds?	Set to **Yes** to raise an event if discovery is partially successful. The details of the event contain the list of discovered devices and the discovery errors that occurred.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which discovery partially succeeds. The default is 15. A partial discovery occurs if only some of the SNMP devices are discovered, or if the maximum device limit is reached. The event message indicates any duplicate IP addresses or hostnames. Duplicates are not considered errors.
Raise event if discovery fails?	Set to **Yes** to raise an event if no SNMP devices are discovered. The details of the event contain the discovery errors that occurred.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no SNMP devices are discovered. The default is 10.

Chapter 65
SNMPUNIX Knowledge Scripts

The SNMPUNIX category provides a set of Knowledge Scripts for monitoring SNMP-enabled devices.

From the Knowledge Script view of Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Many SnmpUNIX Knowledge Scripts use the terms "ODE" and/or "OID":

- **ODE**: SNMP Object Description in its readable, named format. For example, "`system.sysDescr.0`" is the ODE for the numeric OID "`.1.3.6.1.2.1.1.0`".
- **OID**: SNMP Object Identifier in its numeric format. For example, "`.1.3.6.1.2.1.1.0`" is the OID for the SNMP attribute "`system.sysDescr.0`".

Note Many parameters have the option to supply a numeric OID. Numeric OIDs can be supplied in two different formats. If the OID is fully qualified, it must have a leading dot to indicate that the OID is starting from the top of the MIB tree. For example, to specify "`sysUpTime.0`" with a fully qualified numeric OID must include the leading dot as follows: "`.1.3.6.1.2.1.1.3.0`". If a leading dot is not supplied, it is assumed that the numeric OID is preceded by "`iso.org.dod.internet.mgmt.mib.`". Thus, entering an OID of "`1.3.0`" would be translated to: "`iso.org.dod.internet.mgmt.mib.1.3.0`", which is the equivalent of "`sysUpTime.0`" and "`.1.3.6.1.2.1.1.3.0`".

The SNMP category includes the following Knowledge Scripts:

Knowledge Script	What It Does
AddMIBs	Copies the specified list of MIB files to the AppManager agent host where you installed AppManager for SNMP. Reloads the MIB tree for the module so that the new MIBs are recognized.
DeviceReboot	Monitors device uptime for an SNMP device and raises an event if the device has restarted since the last monitoring interval.
InterfaceState	Monitors the contents of the Interface MIB from an SNMP device and raises an event when an interface changes state.
RemoveMIBs	Removes the specified list of MIB files from the AppManager agent host where you installed AppManager for SNMP. Reloads the MIB tree for the module so that the removed MIBs are no longer accessible.
SyncGet	Attempts an SNMP `Get` or `GetNext` for the specified SNMP attributes. Thresholds can be checked, and mathematical conversions can be performed.
SyncGetTable	Retrieves a specified set of SNMP table columns, and reports results for each row retrieved. Thresholds can be checked, and mathematical conversions can be performed.

Knowledge Script	What It Does
SyncPoll	Polls specified SNMP attributes at a prescribed time interval and number of polling attempts. Thresholds can be checked, and mathematical conversions can be performed.
SyncPollTable	Polls a specified set of SNMP table columns at a prescribed time interval and number of polling attempts, and reports summary results for each row polled. Thresholds can be checked, and mathematical conversions can be performed.
SyncSet	Attempts an `SNMP Set` for the specified SNMP attributes of the specified values.

AddMIBs

Use this Knowledge Script to install one or more additional MIB files to an SNMP proxy agent. The specified files are copied to a well-known MIBs directory for the SNMP module, and the module reloads the MIB tree so that the new MIBs take effect.

The default well-known directory is as follows (note that the base directory location may vary, depending on where the agent is actually installed):

This script should be executed when no other SNMP scripts are active on the target proxy agent, because reloading the MIB tree can only be done when no SNMP sessions are active. If this script is unable to reload the MIB tree because of active SNMP sessions, an appropriate event can be raised. If no path or MIB files are supplied, by default this script creates an event containing a list of currently installed MIBs.

Notes

- This script does not transfer the specified MIB files over the network. The directory path specified for the MIB files must already be locally accessible by the SNMP proxy agent.
- SNMP MIBs tend to be organized hierarchically. One MIB is often dependent on another, from which it imports more generic data definitions. This being the case, a MIB should only be added to if all dependent MIBs are already present or are supplied in the same execution of this script.

Tip When is installed, two copies of the supplied MIB files are provided. These files are installed in the following directories assuming that the agent is installed in the default location:

actively uses the MIB files in the directory, but the files in the directory are never modified.

If you accidentally delete one of the original MIB files, for example, by running the RemoveMIBs Knowledge Script, you can recover it from the backup directory. Simply edit the **Full MIB file path** parameter and supply the path to the directory.

If the specified MIB files cannot be found, or an `ASN.1` compilation error occurs while reloading the MIB tree, appropriate error events can be raised.

Resource Object

SNMP Proxy Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Full MIB file path	Enter the directory path where the MIB files to be installed are located. This path must be locally accessible to the SNMP proxy agent.
List of MIB files	Supply a list of MIB filenames without the directory path.
Reload MIB tree?	Set to **Yes** to reload the MIB tree after MIB files have been copied. A MIB tree reload is only attempted if all MIB files are installed successfully.

Parameter	How to Set It
MIB reload timeout	Specify how long the Knowledge Script should wait to try and reload the MIB tree. This can only be performed if no other Knowledge Scripts have active SNMP sessions. The default is 10 seconds.
Event Notification	
Raise event if installation of MIBs succeeds?	Set to **Yes** to raise an event if all MIBs are installed successfully. The details of the event contain the list of installed MIB files.
Event severity when installation of MIBs succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB installation succeeds. The default is 25.
Raise event if installation of MIBs fails?	Set to **Yes** to raise an event if any MIB files fail to install. This can occur if the path of MIB filenames specified is incorrect.
Event severity when installation of MIBs fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB installation fails. The default is 10.
Raise event if reloading of MIB tree succeeds?	Set to **Yes** to raise an event if all MIB files install successfully and the MIB tree is reloaded successfully. This can only occur if the **Reload MIB tree?** parameter is enabled.
Event severity when reloading of MIB tree succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB tree reloading is successful. The default is 25.
Raise event if reload MIB parser warnings received?	Set to **Yes** to raise an event if all MIB files install successfully and reloading the MIB tree reports `ASN.1` parsing errors. This can only occur if the **Reload MIB tree?** parameter is enabled. Details of the parsing errors are in the event.
Event severity when reload MIB parser warnings received	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MIB reload generates warnings. The default is 15.
Raise event if reloading of MIB tree fails?	Set to **Yes** to raise an event if all MIB files install successfully and reloading the MIB tree fails. This can occur if **Reload MIB tree?** is enabled and the **MIB reload timeout** expires.
Event severity when reloading of MIB tree fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB tree reload fails. The default is 10.

DeviceReboot

Use this Knowledge Script to monitor whether SNMP devices reboot. This script tracks the value of `sysUpTime.0` across job iterations to determine whether devices have rebooted. If the value of `sysUpTime.0` is less than the last iteration, the device has either rebooted or the `sysUpTime.0` `TimeTicks` counter value has wrapped.

Before running this script, make sure you have configured AppManager Security Manager with the SNMP information that provides access to the SNMP devices.

The script attempts to track `sysUpTime.0` on all SNMP devices where the script is dropped, regardless of whether any previous attempts have failed. If failures do occur, successful retrievals on other devices are not discarded.

This script collects data streams for each SNMP device. The data value saved is the current number of hours the device has been up.

Resource Objects

SNMP Device objects

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
SNMP Parameters	
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Collect data for device uptime?	Set to **Yes** to collect data for use in graphs and reports. If data collection is enabled, returns the device uptime in hours. By default, data is not collected.
Event Notification	
Raise event if device has rebooted?	Set to **Yes** to raise an event if a device reboot is detected. The details of the event contain the retrieved data.
Event severity when device has rebooted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a device reboots. The default is 15.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise an event if the SNMP `Get` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout threshold is exceeded. The default is 15.
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP Response error is received from the device. The type of error is reported in the event details.

Description	How to Set It
Event severity when SNMP Response error received	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.
Raise event if device uptime baseline established?	Set to **Yes** to raise an event when initial data values are retrieved, setting the baseline for comparison on the next retrieval.
Event severity when device uptime baseline established	Set the event severity level, from 1 to 40, to indicate the importance of an event in which baseline is established. The default is 25.

InterfaceState

Use this Knowledge Script to monitor the state of all interfaces in a device. This is accomplished by tracking the values of `ifAdminStatus` and `ifOperStatus` for each interface across job iterations. If the operational status of an interface changes, an event is created reporting the time that the change occurred. This script also checks to be sure that `ifAdminStatus` and `ifOperStatus` are in sync.

Before running this script, make sure you have configured AppManager Security Manager with the SNMP information that provides access to the SNMP devices.

The script attempts to track interface state on all SNMP devices on which the script is dropped, regardless of whether any previous attempts failed. If failures do occur, successful retrievals on other devices are not discarded.

This script collects separate data streams for each interface in a device. The data value saved is an integer representing the current operational state of each interface.

Resource Objects

This Knowledge Script can be dropped on one or more SNMP Device objects.

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
SNMP Parameters	
List of interface indices	By default, all interfaces are monitored. However, supplying a list of SNMP interface indices can restrict monitoring to those specific interfaces. Indices must be a single integer value. For example, "`1 4 7`" monitors only interfaces with an SNMP interface index of 1, 4 and 7.
Maximum number of interfaces to monitor	Specify the maximum number of interfaces that should be monitored. The default is 100.
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Collect data for interface state?	Set to **Yes** to collect data for use in graphs and reports. If enabled, returns a data stream for each interface in the device indicating its state. By default, data is not collected.
Event Notification	
Raise event if interface state mismatch detected?	Set to **Yes** to raise an AppManager event if an interface has values for `ifAdminStatus` and `ifOperStatus` that are not the same. The details of the event contain the retrieved data.

Parameter	How to Set It
Event severity when interface state mismatch detected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Interface State Mismatch exists. The default is 10.
Raise event if interface state is up?	Set to **Yes** to raise an AppManager event if an interface has transitioned to the Up state since the last Knowledge Script iteration. The details of the event contain the retrieved data.
Event severity when interface state is up	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the interface state is Up. The default is 25.
Raise event if interface state is down?	Set to **Yes** to raise an event if an interface has transitioned to the Down state since the last Knowledge Script iteration. The details of the event contain the retrieved data.
Event severity when interface state is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the interface state is Down. The default is 15.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout is exceeded. The default is 15.
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP Response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.
Raise event if interface state baseline established?	Set to **Yes** to raise an event when initial data values are retrieved, setting the baseline for comparison on the next retrieval.
Event severity when interface state baseline established	Set the event severity level, from 1 to 40, to indicate the importance of an event in which baseline is established. The default severity level is 25.

RemoveMIBs

Use this Knowledge Script to remove one or more MIB files from an SNMP proxy agent. The specified files are deleted from the install directory. The default location is as follows:

This script should be executed when no other SNMP Knowledge Scripts are active on the target AppManager for SNMP installation because reloading the MIB tree can only be done when no SNMP sessions are active. If the RemoveMIBs Knowledge Script is unable to reload the MIB tree because of active SNMP sessions, the script can raise an appropriate event.

Note SNMP MIBs tend to be hierarchical. That is, one MIB is often dependent on another, from which it imports more generic data definitions. This being the case, a MIB should only be deleted if it has no other dependent MIBs installed.

Tip When is installed, two copies of the supplied MIB files are provided. These files are installed in the following directories:

The module actively uses the MIB files in the directory, but the files in the directory are never modified.

If you accidentally delete one of the original MIB files, for example, by running this script, you can recover it from the backup directory. To do this, run the SNMP_AddMIBs Knowledge Script. Edit the **Full MIB File Path** parameter in that Knowledge Script to supply the path to the directory.

If the specified MIB files cannot be deleted, or an `ASN.1` compilation error occurs while reloading the MIB tree, this script can return appropriate error events.

Resource Object

SNMP Proxy Agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
List of MIB files to uninstall	Supply a list of MIB filenames to be deleted.
Reload MIB tree?	Set to **Yes** to reload the MIB tree after MIB files have been deleted. A MIB tree reload is only be attempted if all MIB files are deleted successfully.
MIB reload timeout	Specify how long the Knowledge Script should wait to try and reload the MIB tree. This can only be performed if no other Knowledge Scripts have active SNMP sessions. The default is 10 seconds.
Event Notification	
Raise event if uninstallation of MIBs succeeds?	Set to **Yes** to raise an event if all MIBs are deleted successfully. The details of the event contain the list of installed MIB files.
Event severity when uninstallation of MIBs succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB uninstallation succeeds. The default is 25.

Parameter	How to Set It
Raise event if uninstallation of MIBs fails?	Set to **Yes** to raise an event if any MIB files fail to delete. This can occur if any specified MIB filenames correspond to files not currently installed.
Event severity when uninstallation of MIBs fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB uninstallation fails. The default is 10.
Raise event if reloading of MIB tree succeeds?	Set to **Yes** to raise an event if all MIB files uninstall successfully and the MIB tree is reloaded successfully. This can only occur if the **Reload MIB tree?** parameter is set to Yes.
Event severity when reloading of MIB tree succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB tree reload succeeds. The default is 25.
Raise event if reload MIB parser warnings received?	Set to **Yes** to raise an event if all MIB files uninstall successfully and reloading the MIB tree reports `ASN.1` parsing errors. This can only occur if the **Reload MIB tree?** parameter is set to Yes. Details of the parsing errors are in the event.
Event severity when reload MIB parser warnings received	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB reload warnings are received. The default is 15.
Raise event if reloading of MIB tree fails?	Set to **Yes** to raise an event if all MIB files uninstall successfully but reloading the MIB tree fails. This can occur if the **Reload MIB tree?** parameter is set to Yes and the **MIB Reload timeout** expires.
Event severity when attempt to reload MIB tree fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which MIB tree reload fails. The default is 10.

SyncGet

Use this Knowledge Script to perform an SNMP `Get` or `GetNext` operation for one or more SNMP attributes from one or more SNMP enabled devices. The retrieved values can be compared to thresholds or an equality check can be performed (numeric or string), and AppManager events can be raised if violations occur.

Before running this script, make sure you have configured AppManager Security Manager with the SNMP information that provides access to the SNMP devices.

The script attempts to get the specified attributes on all supplied SNMP devices, regardless of whether any previous attempts failed. If failures do occur, successful gets on other devices are not discarded.

This script can independently collect separate data streams for each SNMP device/SNMP attribute pairing. Thus, the total number of data streams collected is the number of devices the script has been dropped on in the TreeView multiplied by the number of SNMP attributes provided.

Note You must supply either all-numeric SNMP attributes or all-string SNMP attributes, since either a numeric check or string check must be chosen. SNMP attributes that are octet strings, OIDs, or IP addresses are considered to be string attributes.

If one or more numerical conversions are selected, they are performed in the following order: Multiplication, Division, Delta and Percentage. If Delta and Division are both selected, integer division is performed and any remainder is discarded. If Delta is not selected, real-number division is performed.

Values reported in SNMP Success events show the results of multiplication and division conversions, but not delta and percentage conversions, as these are performed after the Success event has been raised. The final result of all conversions is shown in any threshold events, or in the data points if data is collected.

This script can be run at intervals to periodically poll SNMP attributes. However, if delta calculations are being performed on the retrieved values, NetIQ Corporation recommends that the script interval not be less than 1 minute, as the accuracy of delta calculations is time dependent and may not produce reliable results at shorter intervals. This is due to many factors including the accuracy of AppManager job scheduling and network traffic delay. The SyncPoll script should be used to accurately poll at intervals of less than 1 minute.

Notes

- Delta calculations are not normalized. Thus, it is usually necessary to perform a Division conversion on delta calculations to convert to the desired time units. For example, if the growth of an SNMP counter is being tracked by doing a delta calculation at a script interval of 1 minute, it is necessary to divide by 60 to track the growth of the counter on a per-second basis.
- If the **Calculate delta for numeric OID value** parameter is enabled, **integer** math (not **floating point** math) is used; thus, any remainder is discarded.

By default, this script retrieves `sysUpTime.0` from the device, converts the retrieved value to "Days", and reports the retrieved value in a success event.

Resource Objects

One or more SNMP Device objects

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Get Parameters	
SNMP ODE/OIDs	Supply a list of SNMP Attribute ODEs and/or OIDs. ODEs can only be used if the SNMP proxy agent has the corresponding MIB available. The default value is `sysUpTime.0`.
SNMP port number	Supply the UDP port number to send the SNMP request at each SNMP device. The default value is 161.
SNMP retries	Specify the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Specify the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Perform GetNext instead of Get?	Set to **Yes** to perform an SNMP `GetNext` operation instead of a `Get`. The default is to perform a `Get` operation.
OID Value Check	
Collect data for OID value?	Set to **Yes** to collect data for use in graphs and reports. If enabled, returns a data stream for each SNMP device/SNMP attribute pair. By default, data is not collected.
Calculated units	If the Knowledge Script is performing numeric conversions, a name for the resulting units calculated can be entered here. If nothing is supplied for this parameter, the default units are the name of the data type retrieved. The default value is “Days”.
Calculate delta for numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and a delta should be calculated. The difference between the new value and the previous value is calculated. Normally this is used to monitor growth of SNMP counter values between iterations. By default, a delta calculation is not performed. **Note** NetIQ Corporation recommends that you disable this option for Knowledge Script intervals of less than 1 minute. The results may not be reliable.
Use multiplier for numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and should be multiplied by the value specified for the next parameter. By default, multiplication of retrieved values is not performed.
Multiplier value	If the **Use multiplier for numeric OID value?** parameter is enabled, the retrieved SNMP attributes are multiplied by this value before being reported. The default value is 1.
Use divisor for numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and should be divided by the value specified for the next parameter. If you enabled the **Calculate delta for numeric OID value** parameter, integer division is performed and any remainder is discarded. Otherwise, values are converted to real numbers to perform the division and retain the precision of any remainder. By default, division is performed on retrieved values.
Divisor value	If the **Use divisor for numeric OID value?** parameter is enabled, the retrieved SNMP attributes are divided by this value before being reported. The default value is `8640000`.

Parameter	How to Set It
Calculate percentage of numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and should be converted to a percentage of the maximum value supplied in the next parameter. Values are converted to real numbers to perform the percentage calculation and retain the precision of any remainder. Calculated values are restricted to a real number between 0% and 100%. By default, a percentage calculation is not performed on retrieved values.
Maximum value	If the **Calculate percentage of numeric OID value?** parameter is enabled, the retrieved SNMP attributes are converted to a percentage of the maximum value entered here. The default value is 100.
Raise event when maximum threshold exceeded?	Set to **Yes** to specify that the retrieved values should be compared against the maximum threshold value supplied in the next parameter. By default, a threshold check is not performed. If enabled, the check is performed after any mathematical conversions that may have been selected above.
Threshold -- Maximum OID value (post-calculation)	This parameter has no effect unless **Raise event when maximum threshold exceeded?** is enabled. For numeric attributes, specify the maximum threshold value. If this value is exceeded, an event is raised. The threshold value is restricted to whole integer values. The default value is 1000.
Raise event when minimum threshold not met?	Set to **Yes** to specify that the retrieved values should be compared against the minimum threshold value supplied in the next parameter. By default, a threshold check is not performed. If enabled, the check is performed after any mathematical conversions that may have been enabled above.
Threshold -- Minimum OID value (post-calculation)	This parameter has no effect unless **Raise event if threshold not met?** is enabled. For numeric attributes, specify the minimum threshold value. If this threshold is not met, an event is raised. The threshold value is restricted to whole integer values. The default value is 100.
Raise event when OID not equal to value?	Set to **Yes** to specify that the retrieved values should be compared for equality against the value supplied in the **Numeric equality value** parameter. If enabled, the check is performed after any mathematical conversions that may have been enabled above.
Check for inequality instead of equality?	If **Raise event if value not equal?** is enabled, select the **Yes** check box to specify that the retrieved value(s) should be compared for inequality rather than equality.
Numeric equality value	This parameter has no effect unless **Raise event if value not equal?** is enabled. An AppManager event is raised if the retrieved SNMP values equal this value. If **Check Inequality instead of Equality?** is enabled, an event is raised if the retrieved SNMP values are not equal to this value. This threshold is restricted to whole integer values. The default value is 0.
Raise event when string not equal to value?	Set to **Yes** to specify that the retrieved values should be compared for equality against the value supplied in the **String equality value** parameter. SNMP attributes that are strings, octet strings, OIDs, or IP addresses can be checked with a string comparison.
Check for inequality instead of equality?	If **Raise event when string not equal to value?** is enabled, set to **Yes** to specify that the retrieved values should be compared for inequality rather than equality.
Do case-insensitive comparison?	If **Raise event when string not equal to value?** is enabled, set to **Yes** to specify that the retrieved values should be compared without regard to character case.

Parameter	How to Set It
String equality value	If **Raise event when string not equal to value?** is enabled, an event is raised if the retrieved SNMP values equal this value. If **Check for inequality instead of equality?** is enabled, an event is raised if the retrieved SNMP values are not equal to this value. The default value is "`String Value`".
Event severity when OID value violates check	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is crossed or an equality/inequality check fails. The default is 5.
Event Notification	
Raise event if SNMP operation succeeds?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` operation is successful. The details of the event contain the retrieved data.
Event severity when SNMP operation succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMP operation succeeds. The default is 25.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout period is exceeded. The default is 15.
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP Response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.
Raise event if delta baseline established?	This event can be raised only if the **Calculate delta for numeric OID value?** parameter is enabled. Set to **Yes** to raise an event when the initial value is retrieved, setting the baseline for a difference calculation on the next job iteration.
Event severity when delta baseline established	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a delta baseline is established. The default is 25.

SyncGetTable

Use this Knowledge Script to perform an SNMP table walk along specified columns of an SNMP table. The retrieved values can be compared to thresholds or an equality check can be done, and AppManager events can be raised if violations occur.

Note Because this Knowledge Script walks an SNMP table, it is normally not necessary to supply an index value on the ODE/OIDs. Supplying just the attribute name (for example, "`ifDescr`") is normally sufficient. If only a portion of the table is to be walked, a parameter is available to specify the subset of table indices to walk.

The table walk is performed with iterative `GetNext` operations. As soon as any of the attributes walk beyond the end of the table, or the table indices become out of sync, the table walk terminates. If a table is fully populated, all attributes (or table columns) walk beyond the end of the table on the same `GetNext` operation. However, if the table has missing values, the table indices will become out of sync as soon as a missing value is reached. A table walk is terminated when the first missing value is detected.

Before running this script, make sure you have configured AppManager Security Manager with the SNMP information that provides access to the SNMP devices.

This script attempts to walk the specified attributes on all SNMP devices on which the Knowledge Script has been dropped, regardless of whether any previous attempts failed. If failures do occur, successful walks on other devices are not discarded.

This Knowledge Script individually collects separate data streams for each SNMP device/data OID pairing. Thus, the total number of data streams collected is the number of devices the Knowledge Script is dropped on multiplied by the number of data OIDs and the number of rows in the table on each device.

Note You must supply either all-numeric SNMP attributes or all-string SNMP attributes because you must select either a numeric check or string check. SNMP attributes that are octet strings, OIDs, or IP addresses are considered to be string attributes.

If one or more numerical conversions are selected, they are performed in the following order: Multiplication, Division, Delta and Percentage. If Delta and Division are both enabled, integer division is performed, and any remainder is discarded. If Delta is not enabled, real-number division is performed.

Values reported in SNMP Success events show the results of multiplication and division conversions, but not delta or percentage conversions, as these are performed after the Success event has been raised. The final result of all conversions is shown in any threshold-crossing events or reflected in the data streams if data is collected.

This script can be run at intervals to periodically poll SNMP tables. However, if delta calculations are being performed on the retrieved values, NetIQ Corporation recommends that the script interval not be less than 1 minute, as the accuracy of delta calculations is time dependent and may not produce reliable results at shorter intervals. This is due to many factors including the accuracy of AppManager job scheduling and network traffic delay. The SyncPollTable Knowledge Script should be used to accurately poll at intervals of less than one minute.

Note Delta calculations are not normalized. Thus, it is usually necessary to perform a division conversion on delta calculations to convert to the desired time units. For example, if the growth of an SNMP counter is being tracked by doing a delta calculation at a script interval of one minute, it is necessary to divide by 60 to track the growth of the counter on a per second basis. If the **Calculate delta for numeric OID value** parameter is enabled, **integer** math (not **floating point** math) is used, thus any remainder is discarded.

By default, this Knowledge Script retrieves the operational status for all interfaces on a device.

Resource Objects

SNMP Device objects

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Get Table Parameters	
Descriptive ODE/OIDs	Supply a list of SNMP attribute ODEs and/or OIDs. These are descriptive attributes only, which are reported in event and data details for reference purposes. No processing is performed on the retrieved values. The attributes chosen should uniquely identify the retrieved row of an SNMP Table. The default value is "`ifIndex, ifDescr`", which identifies the row number and name of a communications interface in the device.
Data ODE/OIDs	Supply a list of SNMP attribute ODEs and/or OIDs. ODEs can only be used if the SNMP proxy agent has the corresponding MIB available. The default value is `ifOperStatus`.
Optional table indices	By default, the entire SNMP table is walked. However, supplying a list of the table indices that are to be walked can restrict the walk. Indices can be a single integer value, or multiple integer values separated by dots; just like a numeric OID value but without a leading dot. For example, "1.10.42.1.47" is a valid table index.
Maximum number of table rows to get	Specify the maximum number of table rows that should be retrieved. The default is 100.
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
OID value check	
Collect data for OID value?	Set to **Yes** to collect data for graphs and reports. The data is stored in the AppManager repository. When enabled, returns a data stream for each SNMP device/SNMP attribute pair. By default, data is not collected.
Calculated units	If the Knowledge Script is performing numeric conversions, a name for the resulting units calculated can be entered here. If nothing is supplied for this parameter, the default units are the name of the data type retrieved. The default value is nothing.
Calculate delta for numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and the difference between the new value and the previous value should be calculated. Normally this is used to monitor growth of SNMP counter values between iterations. By default, a delta calculation is not performed. **Note** NetIQ Corporation recommends that you not enable this option if monitoring jobs are running at intervals of less than one minute, or the results may not be reliable.

Parameter	How to Set It
Use multiplier for numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and should be multiplied by the value in the next parameter. By default, multiplication is not performed on retrieved values.
Multiplier value	If the **Use multiplier for numeric OID value?** parameter is enabled, the retrieved SNMP attributes are multiplied by this value before being reported. The default value is 1.
Use divisor for numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and should be divided by the value in the next parameter. If the **Calculate delta for numeric OID value** parameter has also been enabled, integer division is performed and any remainder is discarded. Otherwise, values are converted to real numbers to perform the division and retain the precision of any remainder. By default, division is not performed on retrieved values.
Divisor value	If the **Use divisor for numeric OID value?** parameter is enabled, the retrieved SNMP attributes are divided by this value before being reported. The default value is 1.
Calculate percentage of numeric OID value?	Set to **Yes** to specify that the retrieved values are numeric and should be converted to a percentage of the **Maximum value**. Values are converted to real numbers to perform the percentage calculation and retain the precision of any remainder. Calculated values are restricted to a real number between 0% and 100%. By default, percentage calculation is not performed on retrieved values.
Maximum value	If the **Percentage of numeric OID value?** parameter is enabled, the retrieved SNMP attributes are converted to a percentage of the maximum value entered here. The default value is 100.
Raise event when maximum threshold exceeded?	Set to **Yes** to specify that the retrieved values should be compared against the maximum threshold value supplied in the next parameter. By default, a threshold check is not performed. If enabled, the check is performed after any mathematical conversions that may have been selected above.
Threshold -- Maximum OID value (post-calculation)	This parameter has no effect unless **Raise event if threshold exceeded?** is enabled. For numeric attributes, specify the maximum threshold value. If this value is exceeded, an event is raised. The threshold value is restricted to whole integer values. The default value is 1000.
Raise event when minimum threshold not met?	If **Raise event if threshold not met?** is enabled, set to **Yes** to specify that the retrieved values should be compared against the minimum threshold value supplied in the next parameter. By default, a threshold check is not performed. If enabled, the check is performed after any mathematical conversions that may have been selected above.
Threshold -- Minimum OID value (post-calculation)	If the **Raise event if threshold not met?** parameter is enabled, specify a minimum value for numeric attributes after any calculations have been performed. If this threshold is not met, an event is raised. The threshold value is restricted to whole integer values. The default value is 100.
Raise event when OID not equal to value?	Set to **Yes** to specify that the retrieved values should be compared for equality against the value supplied in the **Numeric equality value** parameter. If enabled, the check is performed after any mathematical conversions that may have been selected above.
Check for inequality instead of equality?	If the **Raise event for numeric equality violation?** parameter is enabled, set to **Yes** to specify that the retrieved values should be compared for inequality rather than equality.

Parameter	How to Set It
Numeric equality value	This parameter has no effect unless **Raise event for numeric equality violation?** is enabled. An event is raised if the retrieved SNMP values equal this value. If the **Check for inequality instead of equality?** parameter is enabled, an event is raised if the retrieved SNMP values are not equal to this value. This threshold value is restricted to whole integer values. The default value is 0.
Raise event when string not equal to value?	Set to **Yes** to specify that the retrieved values should be compared for equality against the value supplied in the **String equality value** parameter. SNMP attributes that are strings, octet strings, OIDs, or IP addresses can be checked with a string comparison.
Check for inequality instead of equality?	If the **Raise event for string equality violation?** parameter is enabled, set to **Yes** to specify that the retrieved values should be compared for inequality rather than equality.
Do case-insensitive comparison?	If the **Raise event for string equality violation?** parameter is enabled, set to **Yes** to specify that the retrieved values should be compared for without regard to character case.
String equality value	If the **Raise event for string equality violation?** parameter is enabled, an event is raised if the retrieved SNMP values equal this value. If **Check inequality instead of equality?** is enabled, an event is raised if the retrieved SNMP values are **not equal** to this value. The default value is “String Value”.
Event severity when OID value violates check	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is crossed or an equality/inequality check fails. The default is 5.
Event Notification	
Raise event if SNMP operation succeeds?	Set to **Yes** to raise events if the SNMP `Get` or `GetNext` operation is successful. The details of the event contain the retrieved data.
Event severity when SNMP operation succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMP operation succeeds. The default is 25.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise events if the SNMP `Get` or `GetNext` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout period is exceeded. The default is 15.
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP Response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.
Raise event if delta baseline established?	If **Calculate delta for numeric OID value?** has been enabled, set to **Yes** to raise an event when the initial value is retrieved, setting the baseline for a difference calculation on the next retrieval.
Event severity when delta baseline established?	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a delta baseline is established. The default is 25.

SyncPoll

Use this Knowledge Script to poll SNMP attributes on a Device at short time intervals during each Knowledge Script iteration. Only numeric SNMP attributes may be polled. For each set of polled values, this Knowledge Script computes a minimum, maximum, average and standard deviation. These computed values can then be compared to thresholds, and events can be raised if violations occur.

When this script is dropped on multiple devices, they are polled successively, and not simultaneously. To poll devices simultaneously, a different job must be created for each device.

Note The number of **Polling attempts** multiplied by the **Polling interval** and then multiplied by the number of devices on which the Knowledge Script is dropped must not exceed the time interval between Knowledge Script iterations. Attempting to do so causes the Knowledge Script to abort, as the polling would not be able to complete before the next Knowledge Script iteration is due to execute.

Before running this script, make sure you have configured AppManager Security Manager with the SNMP information that provides access to the SNMP devices.

This script continues polling the SNMP device regardless of whether any previous attempts failed. At least two polling attempts must succeed for any meaningful data to be calculated.

This script individually collects separate data streams for each SNMP attribute. By default, this script calculates the percent bandwidth utilization for the first interface listed in the `ifTable` for the SNMP device, assuming that the speed of this interface is standard Ethernet of 100 Megabits/sec. If the speed of this interface is different, the values returned by the default settings are not valid.

If one or more numerical conversions are selected, they are performed in the following order: Delta, Multiplication, Division and Percentage.

When polling growth of SNMP counter values using the Delta option, all values are normalized on a per second basis, regardless of the length of the polling interval. For example, this script can be used to calculate the Kilobytes per second flowing through an interface by polling `ifInOctets` and `ifOutOctets` and dividing the returned values by 1024. The values reported are Kilobytes per second regardless of the length of the polling interval.

Note If the **Calculate delta for polled value** parameter is enabled, **integer** math (not **floating point** math) is used; thus, any remainder is discarded.

Resource Objects

SNMP Device objects

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Polling Parameters	
SNMP ODE/OIDs	Supply a list of SNMP attribute ODEs and/or OIDs. ODEs can only be used if the SNMP proxy agent has the corresponding MIB available. The default value is: `"ifInOctets.1, ifOutOctets.1"`.
Polling interval	Specify the time interval between polling attempts during each Knowledge Script iteration. The default value is 5 seconds.
Polling attempts	Specify the number of polling attempts to perform during each Knowledge Script iteration. The default value is 12. Combined with the default interval of 5 seconds, this means the Knowledge Script by default polls the SNMP device for 1 minute. The minimum value is 2.
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.
SNMP timeout	Specify the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Polled Values Check	
Collect data for polled values?	Set to **Yes** to collect data for use in graphs and reports. The data is stored in the AppManager repository. If enabled, returns a data stream for each SNMP device/SNMP attribute pair. By default, data is not collected.
Polling calculation type	For each set of polled values, the Average, Minimum, Maximum and Standard Deviation are calculated. Use this parameter to select which calculated value serves as the data point.
Calculated units	Specify a name to identify the units being polled and calculated by this Knowledge Script. The default value is "Percent".
Calculate delta for polled value?	Set to **Yes** to specify that the retrieved values should be considered a delta from the value retrieved by the previous polling attempt. The difference between the new value and the previous value is calculated. Normally this is used to monitor growth of SNMP counter values between polling attempts. By default, a delta calculation is performed. **Note** When this parameter is enabled, the Knowledge Script reports one less polling attempt than was specified for **Polling attempts** because the first polling attempt is used to set a baseline for the delta calculations to follow.
Use multiplier for polled value?	Set to **Yes** to specify that the retrieved values are numeric and should be multiplied by the value in the next parameter. By default, multiplication of retrieved values is not performed.
Multiplier value	If the **Use multiplier for numeric OID value?** parameter is enabled, the retrieved SNMP attributes are multiplied by this value before being reported. The default value is 1.
Use divisor for polled value?	Set to **Yes** to specify that the retrieved values should be divided by the value in the next parameter. Values are converted to real numbers to perform the division and retain the precision of any remainder. By default, division is not performed on retrieved values.
Divisor value	If the **Use divisor for numeric OID value?** parameter is enabled, the retrieved SNMP attributes are divided by this value before being reported. The default value is 1.

Parameter	How to Set It
Calculate percentage of polled value?	Set to **Yes** to specify that the retrieved values should be converted to a percentage of the maximum value supplied in the next parameter. Values are converted to real numbers to perform the percentage calculation and retain the precision of any remainder. Calculated values are restricted to a real number between 0% and 100%. By default, a percentage calculation is performed on retrieved values.
Maximum value	If the **Percentage of numeric OID value?** parameter is enabled, the retrieved SNMP attributes are converted to a percentage of the maximum value entered here. The default value is 12500000 bytes (or 100 Megabits) per second.
Raise event when maximum threshold exceeded?	Set to **Yes** to specify that the retrieved values should be compared against the maximum threshold value supplied in the next parameter. By default, a threshold check is not performed. If enabled, the check is performed after any mathematical conversions that may have been selected above.
Threshold -- Maximum OID value (post-calculation)	This parameter has no effect unless **Raise event when maximum threshold exceeded?** is enabled. For numeric attributes, specify the maximum threshold value. If this value is exceeded by a retrieved value after any selected calculations have been performed, an event is raised. Polling threshold values are real numbers. The default value is 90.
Raise event when minimum threshold not met?	Set to **Yes** to specify that the retrieved values should be compared against the minimum threshold value supplied in the next parameter. By default, a threshold check is not performed. If enabled, the threshold check is done after any mathematical conversions that may have been selected above.
Threshold -- Minimum OID value (post-calculation)	This parameter has no effect unless **Raise event when minimum threshold not met?** is enabled. Specify a minimum threshold value. If the retrieved value fails to meet the threshold value after any calculations have been performed, an event is raised. Polling threshold values are real numbers. The default value is 0.
Event severity when polled value violates check	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is crossed or an equality/inequality check fails. The default is 5.
Event Notification	
Raise event if SNMP operation succeeds?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` operation is successful. The details of the event contain the retrieved data.
Event severity when SNMP operation succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an SNMP operation succeeds. The default is 25.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout period is exceeded. The default is 15.
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.

SyncPollTable

Use this Knowledge Script to perform an SNMP table walk along specified columns of an SNMP table. The retrieved table on the device is then polled at short time intervals at every script iteration. Only numeric attributes may be polled. For each table row that is polled this script computes a minimum, maximum, average and standard deviation. These computed values can then be compared to specified thresholds, and events can be raised if violations occur.

Note Because this script walks an SNMP table, it is normally not necessary to supply an index value on the ODE/OIDs. Supplying just the attribute name (for example, "`ifDescr`") is normally sufficient. If only a portion of the table is to be walked, a parameter is available to specify the subset of table indices to walk.

The table walk is performed with iterative `GetNext` operations. As soon as any attribute walks beyond the end of the table, or the table indices become out of sync, the table walk terminates. If a table is fully populated, all attributes (or table columns) walk beyond the end of the table on the same `GetNext` operation. However, if the table has missing values, the table indices become out of sync as soon as a missing value is reached. A table walk is terminated when the first missing value is detected.

When this script is dropped on multiple devices, they are polled successively, not simultaneously. To poll devices simultaneously, create a different job for each device.

Note The number of **Polling attempts** multiplied by the **Polling interval** and then multiplied by the number of devices on which the script is dropped must not exceed the time interval between script iterations. If this value does exceed the interval, the script job aborts because the polling would not be able to complete before the next Knowledge Script job is due to execute.

Before running this script, make sure you have configured AppManager Security Manager with the SNMP information that provides access to the SNMP devices.

The script continues polling, regardless of whether any previous attempts failed. At least two polling attempts must succeed in order to report meaningful data.

This script collects separate data streams for each SNMP table row. Thus, the number of data streams is the number of SNMP data OIDs, multiplied by the number of rows in the table, and multiplied by the number of devices on which the Knowledge Script is dropped. By default, this script polls how many Kilobytes per second are flowing through each interface listed in the `ifTable` for the SNMP device.

If one or more numerical conversions are selected, they are performed in the following order: Delta, Multiplication, Division and Percentage. When polling growth of SNMP counter values using the Delta option, all values are normalized on a per second basis, regardless of the length of the polling interval. For example, as stated above by default this script calculates the Kilobytes per second flowing through all interfaces in the device. The values reported are Kilobytes per second regardless of the length of the polling interval.

Note If the **Calculate delta for polled value** parameter is enabled, **integer** math (not **floating point** math) is used, thus any remainder is discarded.

Resource Object

Host System Folder running an AppManager agent

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Polling Table Parameters	
Descriptive ODE/OIDs	Supply a list of SNMP Attribute ODEs and/or OIDs. These are descriptive attributes only which are reported in event and data details for reference purposes, and no processing is done on the retrieved values. The attributes chosen should uniquely identify the retrieved row of an SNMP table. The default value is "`ifIndex, ifDescr`", which identifies the row number and name of a communications interface in the device.
Data ODE/OIDs	Supply a list of SNMP Attribute ODEs and/or OIDs. ODEs can only be used if the SNMP module on the AppManager agent computer has the corresponding MIB available. The default value is "`ifInOctets,IfOutOctets`".
Optional table indices	By default, the entire SNMP table is walked. However, supplying a list of the table indices that are to be walked can restrict the walk. Indices can be a single integer value, or multiple integer values separated by dots; just like a numeric OID value but without a leading dot. For example, "1.10.42.1.47" is a valid table index.
Maximum number of table rows to poll	Specify the maximum number of table rows that should be polled. The default is 100.
Polling interval	Specify the time interval between polling attempts during each Knowledge Script iteration. The default value is 5 seconds.
Polling attempts	Specify the number of polling attempts to perform during each Knowledge Script iteration. The default value is 12. Combined with the default interval of 5 seconds, this means the Knowledge Script by default polls the SNMP device for 1 minute. The minimum value is 2.
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.
SNMP timeout	Specify the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Polled Values Check	
Collect data for polled values?	Set to **Yes** to collect data for use in graphs and reports. The data is stored in the AppManager repository. When enabled, returns a data stream for each SNMP device/SNMP attribute pair. By default, data is not collected.
Polling calculation type	For each set of polled values, the Average, Minimum, Maximum and Standard Deviation are calculated. Use this parameter to select which calculated value serves as the data point for the retrieved values.
Calculated units	Specify a name to identify the units being polled and calculated by this Knowledge Script. The default value is "Kbytes/Sec".
Calculate delta for polled value?	Set to **Yes** to specify that the retrieved values should be considered a delta from the value retrieved by the previous polling attempt. The difference between the new value and the previous value is calculated. Normally this is used to monitor growth of SNMP counter values between polling attempts. By default, a delta calculation is performed. **Note** When you enabling this parameter, this Knowledge Script reports one less polling attempt than was specified for **Polling attempts**. This is due to the fact that the first polling attempt is used to set a baseline for the delta calculations to follow.

Parameter	How to Set It
Use multiplier for polled value?	Set to **Yes** to specify that the retrieved values are numeric and should be multiplied by the value in the next parameter. By default, multiplication is not performed on retrieved values.
Multiplier value	If **Use multiplier for numeric OID value?** is enabled, the retrieved SNMP attributes are multiplied by this value before being reported. The default value is 1.
Use divisor for polled value?	Set to **Yes** to specify that the retrieved values are numeric and should be divided by the value in the next parameter. Values are converted to real numbers to perform the division and retain the precision of any remainder. By default, division is not performed on retrieved values.
Divisor value	If **Use divisor for numeric OID value?** is enabled, the retrieved SNMP attributes are divided by this value before being reported. The default value is 1.
Calculate percentage of polled value?	Set to **Yes** to specify that the retrieved values are numeric and should be converted to a percentage of the maximum value supplied in the next parameter. Values are converted to real numbers to perform the percentage calculation and retain the precision of any remainder. Calculated values are restricted to a real number between 0% and 100%. By default, percentage calculation is not performed on retrieved values.
Maximum value	If **Calculate percentage of numeric OID value?** is enabled, the retrieved SNMP attributes are converted to a percentage of the maximum value entered here. The default value is 100.
Raise event when maximum threshold exceeded?	Set to **Yes** to specify that the retrieved values should be compared against the maximum threshold value supplied in the next parameter. By default, no threshold check is performed. If enabled, the check is performed after any mathematical conversions that may have been selected above.
Threshold -- Maximum OID value (post-calculation)	If **Raise event when maximum threshold exceeded?** is selected, specify a maximum threshold value. If a retrieved value exceeds the threshold, an event is raised. Polling threshold values are real numbers. The default value is 1000.
Raise event when minimum threshold not met?	Set to **Yes** to specify that the retrieved values should be compared against the minimum threshold value supplied in the next parameter. By default, no threshold check is performed. If enabled, the check is performed after any mathematical conversions that may have been selected above.
Threshold -- Minimum OID value (post-calculation)	If **Raise event when minimum threshold not met?** is enabled, specify a minimum threshold value. If a retrieved value fails to meet this threshold, an event is raised. Polling threshold values are real numbers. The default value is 100.
Event severity when polled value violates check	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is crossed or an equality/inequality check fails. The default is 5.
Event Notification	
Raise event if SNMP operation succeeds?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` is successful. The details of the event contain the retrieved data.
Event severity when SNMP operation succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an SNMP operation is successful. The default is 25.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise an event if the SNMP `Get` or `GetNext` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout interval is exceeded. The default is 15.

Parameter	How to Set It
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP Response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.

SyncSet

Use this Knowledge Script to set one or more SNMP attributes on one or more SNMP-enabled devices to the specified values. The values can be of different types. However, the SNMP proxy agent that executes the script must have the MIB available for the specified attributes even if numeric OIDs are supplied. This is required so that the value types can be determined. If the MIB for the specified attributes is not available, an SNMP `Failure` event occurs. While requiring the MIB to be installed is a restriction, it does allow the flexibility to easily set multiple SNMP attributes of different types from a single Knowledge Script.

Before running this script, make sure you have configured AppManager Security Manager with the SNMP information that provides access to the SNMP devices.

This script attempts to set the specified attributes on all supplied SNMP devices, regardless of whether any or all of the attempts fail. If failures do occur, successful sets on other devices cannot be reversed or backed out.

Collected data for this script is a Boolean value that specifies whether the SNMP `Set` operation failed or succeeded.

Resource Objects

SNMP Device objects

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
SNMP ODE/OIDs	Supply a list of ODEs and/or OIDs. The default value is "`sysContact.0`".
SNMP values (comma-separated)	Supply a comma-separated list of SNMP attribute values. As some SNMP values could be text strings, commas must be used as separators rather than spaces. The list must contain the same number of items as the **SNMP ODE/OIDs** parameter, and should be in the order corresponding to their respective attribute. The default value is "Your System Administrator".
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.
SNMP retries	Specify the number of retries to attempt if a timeout occurs on an SNMP request. The default is 0 retries.
SNMP timeout	Specify the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Set success	
Collect data for Set success?	Set to **Yes** to collect data for use in graphs and reports. The data is stored in the AppManager repository. When enabled, returns a data stream containing a Boolean value representing whether the `Set` request succeeded or failed.

Parameter	How to Set It
Raise event if Set success not equal to threshold?	Set to **Yes** to raise an event if the result of the `Set` request is not equal to the threshold. By default, events are enabled.
Threshold – Set success	Set this value to one of the following: • 1 -- the `Set` request succeeds • 0 -- the `Set` request does not succeed. The default is 1 (success).
Event severity when Set success not equal to threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Set success is not equal to the threshold you set. The default is 15.
Event Notification	
Raise event if SNMP operation succeeds?	Set to **Yes** to raise an event if the SNMP `Set` operation is successful. The details of the event contain the list of attributes that were set.
Event severity when SNMP operation succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMP `Set` operation succeeds. The default is 25.
Raise event if SNMP timeout exceeded?	Set to **Yes** to raise an event if the SNMP `Set` request receives no response from the device, and all retries fail.
Event severity when SNMP timeout exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMP timeout interval is exceeded. The default is 15.
Raise event if SNMP Response error received?	Set to **Yes** to raise an event if an SNMP Response error is received from the device. The type of error is reported in the event details.
Event severity when SNMP Response error received	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an SNMP Response error is received. The default is 10.

Chapter 66
SQL Knowledge Scripts

AppManager for Microsoft SQL Server provides the following Knowledge Scripts for monitoring SQL Server Knowledge Scripts run on SQL Server 2000, 2005, 2008, or all three. For more information about the compatibility of each Knowledge Script, see the "Version Compatibility" section of each Knowledge Script topic.

The SQL category of Knowledge Scripts is supported for SQL Server resources installed in *clustered* and *non-clustered* environments. In a clustered environment, AppManager raises error events if failover occurs while jobs are running. These error events are expected results of the failover process and can be safely ignored.

When deciding which Knowledge Scripts to run and the appropriate threshold values to use, consider how other applications you manage are dependent on SQL Server.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
Accessibility	Monitors Microsoft SQL Server and database accessibility.
BackupJob	Monitors Microsoft SQL Server backup jobs.
Bcp	Exports data from a Microsoft SQL Server database and imports the data into another Microsoft SQL Server database.
BlockedProcesses	Monitors the number of blocked SQL Server processes.
CacheHitRatio	Monitors the percentage of time that a requested data page is found in the Microsoft SQL Server data cache.
ClusterOwner	Determines the node ownership of an Exchange Virtual Server that is part of a cluster.
Connectivity	Monitors SQL Server connectivity.
CPUUtil	Monitors the percentage of CPU used by SQL Server processes.
DataGrowthRate	Monitors the data growth and shrinkage rates for each SQL Server database.
DataSpace	Monitors available data space and the percentage of data space being used for each database.
DBGrowthRate	Monitors database growth and shrinkage rates.
DBLocks	Monitors the number of locks per database.
DBMirroring	Monitors the Microsoft SQL Server database mirror performance counters.

Knowledge Script	What It Does
DBMirrorStatus	Monitors the status of each mirrored database (SQL Server 2005 and above).
DbOption	Checks to see how Microsoft SQL Server database options are set.
DBSpace	Monitors the available database space and the percentage of database space being used for each database. Monitored database space includes only data space.
DBStats	Monitors the percentage of used space for data and log files.
ErrorLog	Monitors the Microsoft SQL Server error logs.
ErrorLogEx	Monitors the Microsoft SQL Server error log for search strings created using regular expressions or literal searches.
LockUtil	Monitors the length of time that a user must wait for a lock request.
LogGrowthRate	Monitors log growth and shrinkage rates for each SQL Server database.
LoginFailures	Monitors Microsoft SQL Server login failures.
LogShipping	Monitors log shipping metrics.
LogSpace	Monitors the available log space and log space usage of a database.
MemUtil	Monitors the amount of memory used by SQL Server processes.
MonitorDDL	Monitors Data Definition Language (DDL) statements to check for changes in database schema.
MonitorJobs	Monitors Microsoft SQL Server and reports on jobs that have not completed successfully.
NearFileMaxSize	Monitors the size of database files.
NearMaxConnect	Compares the number of connections used to the maximum number of connections configured for the server.
NearMaxLocks	Compares the current number of locks used to the maximum number of locks configured for the server.
NetError	Monitors the number of packet errors that occurred between the current and previous monitoring interval.
ParseErrors	Monitors Microsoft SQL Server parse error messages.
ProcessingTime	Monitors the response time for T-SQL Server statements and other statements.
RepLatency	Monitors the replication latency in milliseconds.
Replication	Monitors the replication latency in milliseconds, the number of transactions marked for replication, the number of transactions being replicated per second, and the replication agent details.
Report_Accessibility	Generates a report about the accessibility of Microsoft SQL Servers and databases.
Report_CacheHitRatio	Generates a report about the percentage of time requested pages are found in the Microsoft SQL Server data cache.
Report_DatabaseDataSpace	Generates a report about the data space available (in MB) and the percentage of data space being used in SQL databases.
Report_DataSpaceAvailabilitySummary	Generates a summary report about the data space available (in MB) in SQL databases.

Knowledge Script	What It Does
Report_DataSpaceUtilizationSummary	Generates a summary report about the percentage of data space used in SQL databases.
Report_DBSpaceAvailabilitySummary	Generates a summary report about the database space available (in MB) in SQL databases.
Report_DBSpaceAvailable	Generates a report about the database space available (in MB) and the percentage of database space used in SQL databases.
Report_DBSpaceUtilizationSummary	Generates a summary report about the percentage of database space used in SQL databases.
Report_ErrorLogSummary	Generates a summary report about entries in the Microsoft SQL Server error logs.
Report_NearMaxConnect	Generates a report about the number of open connections to Microsoft SQL Servers versus the number of allowable connections.
Report_NearMaxLocks	Generates a report about the number of used locks to Microsoft SQL Servers versus the number of allowable locks.
Report_NetError	Generates a report about the number of network packet errors.
Report_Replication	Generates a report about replication latency, the number of transactions in the transaction log marked for replication, the number of transactions replicated per second by Microsoft SQL Servers, and the replication agent details.
Report_ReplicationLatency	Generates a report about replication latency on your Microsoft SQL Servers.
Report_SpaceAvailability	Generates a report about the data space and database space available and the percentage of data space and database space being used in SQL databases.
Report_SpaceAvailabilitySummary	Generates a summary report about the data space and database space available (in MB) in SQL databases.
Report_SpaceUtilizationSummary	Generates a summary report about the percentage of data space and database space used in SQL databases.
Report_To-Be-ReplicatedTransactions	Generates a report about the number of transactions in the transaction log of the publication database that are marked for replication but not yet replicated.
Report_TopCPUUsers	Generates a report about the total CPU time (in milliseconds) consumed by SQL users and their connections.
Report_TopCPUUsersDetail	Generates a detailed report about each data point collected by SQL_TopCPUUsers.
Report_TopIOUsers	Generates a report about the number of I/O read and write operations by SQL users and their connections.
Report_TopIOUsersDetail	Generates a detailed report about each data point collected by SQL_TopIOUsers.
Report_TopLockUsers	Generates a report about the number of locks held by SQL users and their connections.
Report_TopLockUsersDetail	Generates a detailed report about each data point collected by SQL_TopLockUsers.
Report_TopMemoryUsers	Generates a report about the memory that can be allocated to SQL users and their connections.
Report_TopMemoryUsersDetail	Generates a detailed report about each data point collected by SQL_TopMemoryUsers.

Knowledge Script	What It Does
Report_TopResourceUsers	Generates a report on the total CPU time (in milliseconds) used by SQL users and their connections, the number of I/O read and write operations by SQL users and their connections, number of locks held by SQL users and their connections, and the memory that can be allocated to SQL users and their connections.
Report_TransactionsReplicatedPerSec	Generates a report about the number of transactions replicated per second by Microsoft SQL Servers.
Report_UserConnections	Generates a report about the number of Microsoft SQL Server user connections.
Report_UserConnectionsSummary	Generates a summary report about the number of Microsoft SQL Server user connections.
Report_UserMaxConnections	Generates a report on the number of open connections to Microsoft SQL Servers versus the number of allowable connections, and the number of Microsoft SQL Server user connections.
RepTransactions	Monitors the number of transactions in the transaction log that have not yet been replicated.
RepTranSec	Monitors the number of transactions being replicated per second.
RunSql	Runs T-SQL statements or stored procedures.
ServerDown	Monitors the up or down status of Microsoft SQL Server.
ServerThroughput	Monitors the number of I/O transactions and page reads per second.
SPIDsMonitoring	Monitors Microsoft SQL Server for SPID processes that are running for more than a specified time.
StoredProcRecompiles	Monitors the number of times per second that stored procedures are recompiled.
TopCPUUsers	Monitors the total CPU time used by SQL Server users and their connections.
TopIOUsers	Monitors the number of I/O read and write operations used by SQL Server users and their connections.
TopLockUsers	Monitors the total number of locks held by all the SQL Server users and their connections.
TopMemoryUsers	Monitors the total memory pages allocated to all the SQL Server users and their connections.
TopResourceUsers	Monitors the total CPU time used by Microsoft SQL Server users, the number of I/O read and write operations performed, the total number of locks held by all Microsoft SQL Server users and their connections, and the number of memory pages that can be allocated to all Microsoft SQL Server users and their connections.
UserConnections	Monitors the total number of Microsoft SQL Server user connections.
UserMaxConnection	Monitors the total number of Microsoft SQL Server user connections and the opened connection usage of Microsoft SQL Server.

Accessibility

Use this Knowledge Script to monitor Microsoft SQL Server and database accessibility. This script raises an event if Microsoft SQL Server or a specified database is not accessible. In addition, this script generates data streams for database accessibility.

You can set a timeout to determine how many times the Knowledge Script attempts to contact a server or database.

Notes

- This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.
- This Knowledge Script incorrectly equates stopping a job with stopping the server on which the job is running, and thus returns incorrect values for server uptime and downtime. For example, you run a job with the Accessibility Knowledge Script for two hours and then for some reason stop the job, but not the server. You restart the job again three hours later, and it runs for an additional two hours. Although the server was running continuously for seven hours, the report will show the server downtime as three hours and server uptime as four hours.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data for database accessibility?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following: • **100**--all specified databases are accessible • **50**--some of the specified databases are accessible and some are not • **0**--none of the specified databases is accessible. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. The user name you specify must have permission to access the databases to which you want to check accessibility.

Description	How to Set It
Exclude these objects	Specify the name of any database you want to exclude from monitoring. You can specify multiple databases, separated by commas and no spaces. For example: `master,model,mdb`. These databases are excluded even if dynamic monitoring is not enabled. You can use standard pattern-matching characters when specifying database names. • ***** matches zero or more instances of a character • **?** matches exactly one instance of a character • # matches any single digit from 0 - 9 • **[ ]** matches exactly one instance of any character between the brackets, including ranges **Note** If a database name literally matches the pattern you provide, it will be excluded. For example, if you enter `m*`, the `master`, `model`, and `msdb` databases are not monitored, nor is the database coincidentally titled `m*`.
Exclude loading/restoring databases?	Set to **y** if you want to monitor databases that are in a loading or restoring state. The default is n. **Note**: This Knowledge Script always ignores databases in a mirror or witness role.
Timeout	Specify a timeout period in seconds. The timeout period is the number of seconds to wait for a response before retrying or determining the database is inaccessible. The default is 0 seconds (no waiting period). **Notes** When specifying a timeout that the Knowledge Script continues to wait until it receives a response or the timeout is reached. During this waiting period, other jobs are blocked from execution. Limit your use of this parameter or keep the timeout period to a minimum for regular monitoring jobs. When running this script to troubleshoot a particular problem and not at a regularly scheduled interval, adjust this parameter to allow a longer timeout period.
Number of retries	Specify the number of times to retry connecting to the database before determining the database is inaccessible. The default is 0 (no retry attempts). **Notes** Keep in mind that the Knowledge Script continues waiting until it receives a response or has made the specified number of retry attempts. During this waiting period, other jobs are blocked from execution. Therefore, you should limit your use of this parameter or keep retry attempts to a minimum for regular monitoring jobs. When you are running this script to troubleshoot a particular problem and not at a regularly scheduled interval, you might want to adjust this parameter to allow more retry attempts.
Event severity when database not accessible	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the database is not accessible. The default severity level is 5 (red event indicator).

BackupJob

Use this Knowledge Script to monitor Microsoft SQL Server backup jobs. Microsoft SQL Server backup jobs are important for all administrators. Using this script, administrators can track data backup activities optimally.

On the first job iteration, this script sets a starting point for future log scanning and does not scan the existing entries in the logs. Therefore, it does not return any results on the first iteration. As it continues to run at the interval specified in the Schedule tab, this script scans the logs for any new entries created since the last time it checked.

This script raises an event if the number of successful backup records exceeds the threshold you specify, and if the backup fails for any reason.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if backup job fails?	Set to **Yes** to raise an event if a backup job fails. The default is Yes.
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the backup job fails. The default severity level is 5.
Raise event if threshold is exceeded?	Set to **Yes** to raise an event if the number of backup records exceeds the threshold. The default is Yes.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of backup records exceeds the threshold. Severity level 1 is the highest. The default severity level is 15.
Data Collection	
Collect data for backup jobs?	Set to **Yes** to collect backup jobs data for charts and reports. If enabled, data collection returns the number of successful backup records. The default is Yes.
Custom data stream legend	Specify a legend for the job's data stream.

Description	How to Set It
Monitoring	
Threshold -- Maximum number of successful backup records	Specify the maximum number of successful backup records to be displayed. An event is raised when this number is exceeded. The default number of backup records is 100.

Bcp

Use this Knowledge Script to copy data from one Microsoft SQL Server database table (the source) into another Microsoft SQL Server database table (the destination). This script uses the bulk copy program (BCP) to copy Microsoft SQL Server data to and from an operating system file. This script raises an event if the copy operation fails for any reason.

If the destination Microsoft SQL Server database table does not exist, the job will fail. BCP will not create a table if one does not already exist.

Required SQL Permissions

This Knowledge Script requires a SQL Server user login account that has permission to access the Source and Destination databases and tables.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Once every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Source SQL Server	Specify the name of the Microsoft SQL Server that contains the table you want to export. For example, `sales_nw`. If you do not specify a computer name, the local Microsoft SQL Server is used.
Source SQL Server database name	Specify the name of the database that contains the table you want to export. For example, `master`.
Source SQL Server table name	Specify the name of the table you want to export. For example, `territories`.
Source SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. The user name you specify must have permission to access the source database and table. The default is the "`sa`" user account. **Note** Leave the login and password parameters blank to use Windows authentication. When the parameters are blank, the Knowledge Script performs the BCP command using the credentials as specified for the NetIQ agent service.
Source SQL Server password	Specify the password for the database user account being used to access Microsoft SQL Server.
Destination SQL Server	Specify the name of the Microsoft SQL Server from which you want to import the copied data. For example, `corp_office`.

Description	How to Set It
Destination SQL Server database name	Specify the name of the database to which you want to export the copied data. For example, `sales`.
Destination SQL Server table name	Specify the name of the table to which you want to export the data. For example, `territories`.
Destination SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. The user name you specify must have permission to access the destination database and table. The default is the "`sa`" user account. **Note** Leave the login and password parameters blank to use Windows authentication. When the parameters are blank the Knowledge Script performs the BCP command using the credentials as specified for the NetIQ agent service.
Destination SQL Server password	Specify the password for the database user account being used to access the destination Microsoft SQL Server.
SQL Server "..\Tools" path	Specify the path to the `Tools` directory on the local Microsoft SQL Server computer (where the script is running). The default path (Microsoft SQL Server 2000) is `C:\Program Files\Microsoft SQL Server\80\Tools`. For Microsoft SQL Server 2005, the path is `C:\Program Files\Microsoft SQL Server\90\Tools`. For Microsoft SQL Server 2008, the path is `C:\Program Files\Microsoft SQL Server\100\Tools`. **Note** Generally, you run this script on either the source or destination Microsoft SQL Server computer. However the script does not require that you run it on the source or destination computer as long as the Microsoft SQL Server you choose as the target has access to those computers and to the BCP program.
Event severity when copy operation fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the copy operation fails. The default severity level is 8 (red event indicator).

BlockedProcesses

Use this Knowledge Script to monitor the number of SQL Server processes that are blocked for longer than the period of time you specify. For Microsoft SQL Server 2000 and later, you can set a threshold to determine how long a process in queue before it is considered blocked. This script raises an event when the number of blocked processes exceeds a threshold you set.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every minute**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of blocked processes exceeds threshold?	Set to **y** to raise an event if the number of blocked processes exceeds the threshold. The default is y.
Collect data for number of currently blocked processes?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of currently blocked processes. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "sa" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through the AppManager Security Manager. **Note** The account must be in the `sysadmin` Fixed Server Role.
Threshold -- Maximum time in queue	Specify the maximum length of time a process can be queued before it is considered a blocked process. The default is 500 milliseconds.
Threshold -- Maximum number of blocked processes	Specify the maximum number of processes that can be blocked before an event is raised. The default is 5 blocked processes.
Number of blocked processes to include in event	Specify the number of processes to display in the Graph pane of the Operator Console. The default is 20 blocked processes.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of blocked processes exceeds the threshold. The default severity level is 5 (red event indicator).

CacheHitRatio

Use this Knowledge Script to monitor the percentage of time that a requested data page is found in the Microsoft SQL Server data cache. This script raises an event if the cache hit ratio falls below the threshold you set.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if cache hit ratio falls below threshold?	Set to **y** to raise an event when the cache hit ratio falls below the threshold. The default is y.
Collect data for cache hit ratio?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the cache hit percentage. The default is n.
Threshold -- Minimum cache hit ratio	Specify the minimum percentage of time that requested data pages can be found in the data cache before an event is raised. Ideally this percentage should be set relatively high, because the more frequently Microsoft SQL Server uses the data cache, the better your database performance. When Microsoft SQL Server accesses information in the data cache less frequently than the threshold you set, for example only 50% of the time, an event informs you that database performance has deteriorated. The default is 90%.
Event severity when threshold not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the cache hit ratio falls below the threshold. The default severity level is 5 (red event indicator).

ClusterOwner

Use this Knowledge Script to determine whether a Microsoft SQL Server computer that is part of a cluster is the owner of the node. This script raises an event if the computer is not the current node owner. In addition, this script generates data streams for ownership status.

Note
To use the ClusterOwner script, the agent services, `NetIQccm` and `NetIQmc`, must run using a domain user account.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if not node owner? (y/n)	Set to **y** to raise an event if the selected computer is in a cluster but is not the node owner. The default is y.
Collect data for ownership status? (y/n)	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following: • 100--the computer is a cluster owner or the computer is not in a cluster • 0--the computer is in a cluster but is not the cluster owner. The default is n.
Event severity when not node owner	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the selected computer is not the node owner. The default severity level is 20.
Raise event when node is down? (y/n)	Set to **y** to raise an event if the selected node is down. The default is y.
Severity when the node is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the selected node is down. The default severity level is 5.

Connectivity

Use this Knowledge Script to monitor Microsoft SQL Server connectivity. You can check whether a Microsoft SQL Server instance can be reached. You can also set a timeout to determine the number of times the script should attempt to contact the server.

This script raises an event if, during any monitoring interval, the number of times the server is not available exceeds the number of retries you specify.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitor the server connectivity	
Raise event if connection with the server/instance not possible?	Set to **Yes** to raise an event if the connection with the server/instance is not possible. By default, raising an event is enabled.
Event severity when connection with the server not possible	Set the event severity level, from 1 to 40, to indicate the importance of an event in which connection with the server/instance is not possible. The default is 5.
Data Collection	
Collect data for server connectivity?	Set to **Yes** to collect server connectivity data for charts and reports. The default is Yes.
Custom data stream legend	Specify a custom data stream legend for the job.
Monitoring	
TimeOut	Specify the maximum number of seconds the Connectivity script should wait for a response before retrying. The default is 0 seconds.
Number of retries	Specify the number of times the Connectivity script must retry connecting to the Microsoft SQL Server before determining that the database is inaccessible. The default is 0.

CPUUtil

Use this Knowledge Script to monitor the percentage of CPU resources used by the `sqlservr`, `sqlagent`, and `sqlexec` processes. This script raises an event if the CPU usage for SQL Server processes exceeds the threshold you set.

Note
This script does not raise events or generate data points when you run it on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server

Default Schedule

The default schedule for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if CPU utilization exceeds threshold?	Set to **y** to raise an event if CPU utilization exceeds the threshold. The default is y.
Collect data for CPU utilization?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the CPU resources (as percentages of CPU time) used by SQL Server processes. The default is n.
Threshold -- Maximum CPU utilization for all processes	Specify the maximum percentage of CPU resources that can be consumed by all SQL Server processes before an event is raised. The default is 60%.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU utilization exceeds the threshold. The default severity level is 5 (red event indicator).

DataGrowthRate

Use this Knowledge Script to monitor the data growth and shrinkage rates for all Microsoft SQL Server databases. Monitoring only includes database data files. Growth and shrinkage rates are calculated by taking the difference of the data space utilization during the current monitoring interval from the data space utilization during the previous monitoring interval. This script raises an event if either rate exceeds a threshold you set.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Required SQL Permissions

This Knowledge Script requires a SQL Server user login account that is in the public Fixed Server Role and the `sysadmin` Role. The user login account must also be in the `db_owner` Fixed Database Role for every database where you want to run this Knowledge Script.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Objects

Microsoft SQL Server or Database folder, if dynamically observing databases. If you are not observing databases dynamically, you can run this Knowledge Script on the Database folder or on individual database objects. If you run this script on an individual database object, only that object is monitored regardless of how you set the *Dynamically observe databases at each interval?* parameter.

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe databases at each interval?	Set to **y** to dynamically observe databases at each monitoring interval. The default is y. **Note** Dynamic observation takes place only when the script is run on the Databases object, not when it is run on an individual database.
Exclude these objects	Specify the name of any database you want to exclude from monitoring. You can specify multiple databases, separated by commas and no spaces. For example: `master,model,mdb`. These databases are excluded even if dynamic monitoring is not enabled. You can use standard pattern-matching characters when specifying database names. • ***** matches zero or more instances of a character • **?** matches exactly one instance of a character • # matches any single digit from 0 - 9 • **[ ]** matches exactly one instance of any character between the brackets, including ranges **Note** If a database name literally matches the pattern you provide, it will be excluded. For example, if you enter `m*`, the `master`, `model`, and `msdb` databases are not monitored, nor is the database coincidentally titled `m*`.
Raise event if rate exceeds threshold?	Set to **y** to raise events if growth and shrink rates exceed the threshold. The default is y.
Raise event if database is offline?	Set to **y** to raise events if the database is offline. The default is y.
Collect data for growth and shrinkage rates?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the data growth and shrinkage rates for each database. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the public Fixed Server Role. It must also be in the `db_owner` Fixed Database Role for every database where you want to run this job.
Threshold -- Maximum percentage of data growth	Specify the maximum percentage of data growth that is allowed between the last and current interval before an event is raised. The default is 25%.
Threshold -- Maximum percentage of data shrinkage	Specify the maximum percentage of data shrinkage that is allowed between the last and current interval before an event is raised. The default is 25%.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default severity level is 5 (red event indicator).
Severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an unexpected error occurs. The default is 35.

DataSpace

Use this Knowledge Script to monitor available data space and the percentage of data space being used for each database. Monitored database space includes only data space. This script raises an event if the amount of available data space, in MB, is lower or the percentage of data space used is higher than the thresholds you set.

You can set this script to observe new databases dynamically each time it runs. Observing databases dynamically allows you to monitor data space for databases that have been added since you ran the Discovery_SQL Knowledge Script and prevents you from attempting to monitor databases that have been dropped since discovery.

Notes

- Although this script can observe databases each time it runs, the new databases are not reflected in the Operator Console or Control Center.
- This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Required SQL Permissions

This Knowledge Script requires a SQL Server user login account that is in the public Fixed Server Role and the `sysadmin` Role. The user login account must also be in the `db_owner` Fixed Database Role for every database where you want to run this Knowledge Script.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Objects

Microsoft SQL Server or Database folder, if dynamically observing databases. If you are not observing databases dynamically, you can run this script on the Database folder or individual database objects. If you run the script on a individual database object, only that object is monitored regardless of how you set the *Dynamically observe databases at each interval?* parameter.

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe databases at each interval?	Set to **y** to dynamically observe databases at each monitoring interval. The default is y. **Note** Dynamic observation takes place only when the script is run on the Databases object, not when it is run on an individual database.
Exclude these objects	Specify the name of any database you want to exclude from monitoring. You can specify multiple databases, separated by commas and no spaces. For example: `master,model,mdb`. These databases are excluded even if dynamic monitoring is not enabled. You can use standard pattern-matching characters when specifying database names. • ***** matches zero or more instances of a character • **?** matches exactly one instance of a character • # matches any single digit from 0 - 9 • **[ ]** matches exactly one instance of any character between the brackets, including ranges **Note** If a database name literally matches the pattern you provide, it will be excluded. For example, if you enter `m*`, the `master`, `model`, and `msdb` databases are not monitored, nor is the database coincidentally titled `m*`.
Raise event if threshold exceeded or not met?	Set to **y** to raise an event if a monitored value exceeds or falls below the threshold you set. The default is y.
Raise event if database is offline?	Set to **y** to raise an event if the database is offline. The default is y.
Collect data for available data space and percentage used?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the available data space (in MB) and the percentage of data space used for each database. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the public Fixed Server Role. Also it must be in the `db_owner` Fixed Database Role for every database where you want to run this job.
Threshold -- Minimum available data space	Specify the minimum amount of data space that is required to be available before an event is raised. If the amount of available data space falls below this threshold, an event is raised. The default is 0 MB.
Threshold -- Maximum percentage of data space used	Specify the maximum percentage of data space that can be in use before an event is raised. The default is 90%.
Event severity when threshold exceeded or not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored value exceeds or falls below the threshold. The default severity level is 5 (red event indicator).
Severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event if an unexpected error occurs. The default is 35 (magenta level indicator).

DBGrowthRate

Use this Knowledge Script to monitor database growth and shrinkage rates. Monitoring includes database data and log files. Growth and shrinkage rates are calculated by taking the difference of the database space utilization from the current monitoring interval and the database space utilization from the previous interval. This script raises an event if either rate exceeds the threshold you set.

If you enable the *Recalculate usage?* parameter, this script calls a Microsoft stored procedure that corrects inaccuracies in the `sysindexes` table. These inaccuracies might result in incorrect space usage reports.

Note
This script does not raise events or generate data points when you run it on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Objects

Microsoft SQL Server or Database folder, if dynamically observing databases. If you are not observing databases dynamically, you can run this script on the Database folder or individual database objects. If you run the script on a individual database object, only that object is monitored regardless of how you set the *Dynamic observation* parameter.

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe databases at each interval	Set to **y** to dynamically observe databases at each monitoring interval. The default is y. **Note** Dynamic observation takes place only when the script is run on the Databases object, not when it is run on an individual database.
Exclude these objects	Specify the name of any database you want to exclude from monitoring. You can specify multiple databases, separated by commas and no spaces. For example: `master,model,mdb`. These databases are excluded even if dynamic monitoring is not enabled. You can use standard pattern-matching characters when specifying database names. • ***** matches zero or more instances of a character • **?** matches exactly one instance of a character • # matches any single digit from 0 - 9 • **[ ]** matches exactly one instance of any character between the brackets, including ranges **Note** If a database name literally matches the pattern you provide, it will be excluded. For example, if you enter `m*`, the `master`, `model`, and `msdb` databases are not monitored, nor is the database coincidentally titled `m*`.
Raise event if rate exceeds threshold?	Set to **y** to raise an event if growth and shrink rates exceed the threshold. The default is y.
Raise event if database is offline?	Set to **y** to raise events if a database is offline. The default is y.
Collect data for database growth and shrinkage rates?	Set to **y** to collect data for charts and reports. If enabled, data collection returns database growth and shrinkage rates. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the managed client's Microsoft SQL Server and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the public Fixed Server Role. Also it must be in the `db_owner` Fixed Database Role for every database where you want to run this job.
Recalculate usage?	Set to **y** to have Microsoft SQL Server recalculate the space usage. If enabled, the Knowledge Script calls a Microsoft stored procedure that corrects inaccuracies in the `sysindexes` table, which might result in incorrect space usage reports. The default is n.
Threshold -- Maximum percentage of database growth	Specify the maximum percentage of database growth that is allowed between the previous and current interval before an event is raised. The default is 25%.
Threshold -- Maximum percentage of database shrinkage	Specify the maximum percentage of database shrinkage that is allowed between the previous and current interval before an event is raised. The default is 25%.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which growth and shrink rates exceed the threshold. The default severity level is 5 (red event indicator).

DBLocks

Use this Knowledge Script to monitor the number of locks per database. This script raises an event if the number of locks exceeds the threshold. In addition, this script generates data streams for the number of locks, and you can include information about the number of database locks in the events and data for this script.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Objects

Databases object, or individual databases.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe databases at each interval?	Set to **y** to dynamically observe databases at each monitoring interval. The default is y. **Note** Dynamic observation takes place only when the script is run on the Databases object, not when it is run on an individual database.
Exclude these objects	Specify the name of any database you want to exclude from monitoring. You can specify multiple databases, separated by commas and no spaces. For example: `master,model,mdb`. These databases are excluded even if dynamic monitoring is not enabled. You can use standard pattern-matching characters when specifying database names. • ***** matches zero or more instances of a character • **?** matches exactly one instance of a character • # matches any single digit from 0 - 9 • **[ ]** matches exactly one instance of any character between the brackets, including ranges **Note** If a database name literally matches the pattern you provide, it will be excluded. For example, if you enter `m*`, the `master`, `model`, and `msdb` databases are not monitored, nor is the database coincidentally titled `m*`.
Raise event if locks exceed threshold?	Set to **y** to raise an event when the number of locks for a database exceeds the threshold. The default is y.

Description	How to Set It
Collect data for number of database locks?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of locks held on a database, and identifies the application and user holding each lock. The default is y.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "sa" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager.
Threshold -- Maximum number of database locks	Specify the maximum number of locks that can be held on a database before an event is raised. The default is 10 locks.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of locks held exceeds the threshold. The default severity level is 5 (red event indicator).
Database locks reporting	
Include database locks report in events?	Set to **y** to include a report of the number of database locks in the events generated for this script.The default is y.
Include database locks report in data?	Set to **y** to include a report of the number of database locks in the data for charts and reports.The default is y.
Maximum locks to report (0 for no maximum)	Set the maximum number of locks you want the script to report on for events and data. The default is 0.

DBMirroring

Use this Knowledge Script to monitor the Microsoft SQL Server database mirror performance counters.

Database mirroring is a Microsoft SQL Server 2005 technology that improves database availability. Database mirroring transfers transaction log records directly from one server to another. You can code client applications to automatically redirect their connection information, and in the event of a failover, automatically connect to the standby server and database. Fast failover with minimal data loss has traditionally involved higher hardware cost and greater software complexity. Database mirroring, however, can failover quickly with no loss of committed data.

This script collects information regarding various performance counters and raises events when the various thresholds are exceeded.

Notes

- This script monitors the transaction delay, redo queue value, log send queue and log bytes sent performance counters. It does not monitor other performance counters.
- This script does not work on SQL standalone environments.
- This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2005 and 2008

Resource Objects

Database objects or individual databases

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise Event	
Raise event if bytes received exceeds threshold?	Set to **Yes** to raise an event if the number of bytes received per second exceeds threshold. The default is Yes.
Raise event if bytes sent exceeds threshold?	Set to **Yes** to raise an event if the number of bytes sent per second exceeds threshold. The default is Yes.
Raise event if log bytes received exceeds threshold?	Set to **Yes** to raise an event if the number of log bytes received per second exceeds threshold. The default is Yes.
Raise event if log bytes sent exceeds threshold?	Set to **Yes** to raise an event if the number of log bytes sent exceeds threshold. The default is Yes.

Description	How to Set It
Raise event if log send queue exceeds threshold?	Set to **Yes** to raise an event if the total number of kilobytes of log that have not been sent to the mirror server exceeds threshold. The default is Yes.
Raise event if pages sent exceeds threshold?	Set to **Yes** to raise an event if the number of pages sent per second exceeds threshold. The default is Yes.
Raise event if mirror messages received exceeds threshold?	Set to **Yes** to raise an event if the number of mirroring messages received per second exceeds threshold. The default is Yes.
Raise event if redo bytes received exceeds threshold?	Set to **Yes** to raise an event if the number of bytes of log redone by the mirror database per second exceeds threshold. The default is Yes.
Raise event if redo queue exceeds threshold?	Set to **Yes** to raise an event if total number of kilobytes that redo on the mirror database is behind the hardened log. The default is Yes.
Raise event if packets waited in flow control per second exceeds threshold?	Set to **Yes** to raise an event if the number of milliseconds per second that packets waited in flow control exceeds threshold. The default is Yes.
Raise event if number of sends initiated per second exceeds threshold?	Set to **Yes** to raise an event if the number of sends initiated per second exceeds threshold. The default is Yes.
Raise event if transaction delay exceeds threshold?	Set to **Yes** o raise an event if the average amount of delay experienced by transactions waiting for acknowledgement exceeds threshold. The default is Yes.
Data Collection	
Collect data for bytes received?	Set to **Yes** to collect data points for the number of bytes received per second. The default is Yes.
Collect data for bytes sent?	Set to **Yes** to collect data points for the number of bytes sent per second. The default is Yes.
Collect data for log bytes received?	Set to **Yes** to collect data points for the number of bytes of log received per second. The default is Yes.
Collect data for log bytes sent?	Set to **Yes** to collect data points for the number of bytes of log sent per second. The default is Yes.
Collect data for log send queue?	Set to **Yes** to collect data points for the total number of kilobytes of log that have not been sent to the mirror server. The default is Yes.
Collect data for pages sent?	Set to **Yes** to collect data points for the number of pages sent per second. The default is Yes.
Collect data for mirror messages received?	Set to **Yes** to collect data points for the number of mirror messages received per second. The default is Yes.
Collect data for redo bytes received?	Set to **Yes** to collect data points for the number of bytes of log redone by the mirror database per second. The default is Yes.
Collect data for redo queue?	Set to **Yes** to collect data points for the total number of kilobytes that redo on the mirror database is behind the hardened log. The default is Yes.
Collect data for packets waited in flow control per second?	Set to **Yes** to collect data points for the millisecond packets waited in flow control per second. The default is Yes.
Collect data for number of sends initiated per second?	Set to **Yes** to collect data points for the number of sends initiated per second. The default is Yes.
Collect data for transaction delay?	Set to **Yes** to collect data points for the average delay in transaction termination waiting for acknowledgement. The default is Yes.
Monitoring	

Description	How to Set It
Threshold -- Maximum bytes received per second	Specify the maximum number of bytes that can be received per second before an event is raised. The default is 100. The maximum threshold value is 5000; the minimum threshold value is 0.
Threshold -- maximum bytes sent per second	Specify the maximum number of bytes that can be sent per second before an event is raised. The default is 100. The maximum threshold value is 5000; the minimum threshold value is 0.
Threshold -- maximum log bytes received per second	Specify the maximum number of log bytes that can be received per second before an event is raised. The default is 100. The maximum threshold value is 5000; the minimum threshold value is 0.
Threshold -- maximum log bytes sent per second	Specify the maximum number of log bytes that can be sent per second before an event is raised. The default is 100. The maximum threshold value is 5000; the minimum threshold value is 0.
Threshold -- maximum log send queue	Specify the maximum number of log bytes that can be in the send queue before an event is raised. The default is 100. The maximum threshold value is 5000; the minimum threshold value is 0.
Threshold -- maximum pages sent per second	Specify the maximum number of pages that can be sent per second before an event is raised. The default is 100. The maximum threshold value is 5000; the minimum threshold value is 0.
Threshold -- maximum mirror messages received per second	Specify the maximum number of mirror images that can be received per second before an event is raised. The default is 100. The maximum threshold value is 5000; the minimum threshold value is 0.
Threshold -- maximum redo bytes per second	Specify the maximum number of redo bytes that can occur per second before an event is raised. The default is 100. The maximum threshold value is 5000; the minimum threshold value is 0.
Threshold -- maximum redo queue value	Specify the maximum number of redo bytes that can be in queue before an event is raised. The default is 100. The maximum threshold value is 5000; the minimum threshold value is 0.
Threshold -- maximum packets waiting in flow control per second	Specify the maximum number of packets per second that can be waiting in flow control before an event is raised. The default is 100. The maximum threshold value is 5000; the minimum threshold value is 0.
Threshold -- maximum number of sends initiated per second	Specify the maximum number of sends that can be initiated per second before an event is raised. The default is 100. The maximum threshold value is 5000 while the minimum threshold value is 0.
Threshold -- maximum transaction delay	Specify the maximum amount of transaction delay that can occur before an event is raised. The default is 100. The maximum threshold value is 5000; the minimum threshold value is 0.

DBMirrorStatus

Use this Knowledge Script to monitor the status of each mirrored database. This script raises an event if one of the selected factors associated with the mirrored database changes, such as the mirror state, mirror role, or mirror partner, or if a new database is added or removed from mirroring.

Version Compatibility

Microsoft SQL Server 2005 and 2008

Resource Objects

Microsoft SQL Server

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
KS Settings	
SQL Login	Specify the database user login account needed to access Microsoft SQL Server. Leave this field blank if you want to use Windows Authentication, and the `netiqmc` service is running with the appropriate credentials. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager.
Event Settings	
Raise an event if Mirror State changes?	Set to **Yes** to raise an event if the Mirror State changes. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event if the Mirror State changes. The default severity level is 5 (red event indicator).
Raise an event if Mirror Role changes?	Set to **Yes** to raise an event if the Mirror Role changes. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event if the Mirror Role changes. The default severity level is 5 (red event indicator).
Raise an event if Mirror Role Sequence changes?	Set to **Yes** to raise an event if the Mirror Role Sequence changes. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event if the Mirror Role Sequence changes. The default severity level is 5 (red event indicator).
Raise an event if Mirror Safety Level changes?	Set to **Yes** to raise an event if the Mirror Safety Level changes. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event if the Mirror Safety Level changes. The default severity level is 5 (red event indicator).

Description	How to Set It
Raise an event if Mirror Safety Sequence changes?	Set to **Yes** to raise an event if the Mirror Safety Sequence changes. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event if the Mirror Safety Sequence changes. The default severity level is 5 (red event indicator).
Raise an event if Mirror Partner changes?	Set to **Yes** to raise an event if the Mirror Partner changes. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event if the Mirror Partner changes. The default severity level is 5 (red event indicator).
Raise an event if Mirror Witness changes?	Set to **Yes** to raise an event if the Mirror Witness changes. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event if the Mirror Witness changes. The default severity level is 5 (red event indicator).
Raise an event if Mirror Witness State changes?	Set to **Yes** to raise an event if the Mirror Witness State changes. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event if the Mirror Witness State changes. The default severity level is 5 (red event indicator).
Raise an event if no mirrored databases found?	Set to **Yes** to raise an event if no mirrored databases are found. The default is No.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event if no mirrored databases are found. The default severity level is 25 (blue level indicator).
Raise an event if a new database is mirrored?	Set to **Yes** to raise an event if a new database is mirrored. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event if a new database is mirrored. The default severity level is 25 (blue level indicator).
Raise an event if a database is removed from mirroring?	Set to **Yes** to raise an event if a database is removed from mirroring. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event if a database is removed from mirroring. The default severity level is 5 (red event indicator).
Severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of the event if an unexpected error occurs. The default is 35 (magenta level indicator).

DbOption

Use this Knowledge Script to check how Microsoft SQL Server database options are set. You can select which options to monitor and choose whether to raise an event when a selected option is set (`ON`) or not set (`OFF`).

Note
This script does not raise events or generate data points when you run it on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Database object

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if option is ON?	Set to **y** to raise events when the specified options are set (are `ON`). The default is y.
Raise event if option is OFF?	Set to **y** to raise events when the specified options are not set (are `OFF`). The default is n.
Collect data for options on?	Set to **y** to collect data for charts and reports. If enabled, data collection returns one of the following: • **100**--all of the specified options are on • **50**--some options are on • **0**--no options are on. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager.
Monitor all options?	Set to **y** to check all database options and see whether they are on. The default is y.
ANSI null default option?	Set to **y** to check whether the "ANSI null default" option is on. When set, this database option controls whether database columns are null by default. The default is n.
ANSI nulls option?	Set to **y** to check whether the "ANSI nulls" option is on. When this database option is set to `true`, all comparisons to a null value evaluate to `unknown`. The default is n.

Description	How to Set It
ANSI warnings option?	Set to **y** to check whether the “ANSI warnings” option is on. This database option controls whether errors or warnings are issued when conditions such as “divide by zero” occur. The default is n.
Auto close option?	Set to **y** to check whether the “auto close” option is on. When this database option is set to `true`, the database is shut down cleanly and its resources are freed after the last user exits. The default is n.
Auto create statistics option?	Set to **y** to check whether the “auto create statistics” option is on. When this database option is set to `true`, statistics are automatically created on columns used in a predicate. The default is n.
Auto update statistics option?	Set to **y** to check whether the “auto update statistics” option is on. When this database option is set to `true`, existing statistics are automatically updated when the statistics become out-of-date. The default is n.
Auto shrink option?	Set to **y** to check whether the “auto shrink” option is on. When this database option is set to `true`, the database files are candidates for automatic periodic shrinking. The default is n.
Concat null yields option?	Set to **y** to check whether the “concat null yields” option is on. When this database option is set to `true`, if either operand in a concatenation operation is null, the result is null. The default is n.
Cursor close on commit option?	Set to **y** to check whether the “cursor close on commit” option is on. When this database option is set to `true`, any cursors that are open when a transaction is committed or rolled back are closed. The default is n.
For dbo use only option?	Set to **y** to check whether the “dbo use only” option is on. This database option specifies that only the database owner can access the database. The default is n.
Default to local cursor option?	Set to **y** to check whether the “default to local cursor” option is on. This database option controls whether cursor declarations default to local. The default is n.
Merge publish option?	Set to **y** to check whether the “merge publish” option is on. This database option controls whether the database can be published for a merge replication. The default is n.
Offline option?	Set to **y** to check whether the database is configured for offline operation. The default is n.
Published option?	Set to **y** to check whether the database is configured for publishing (replication). The default is n.
Quoted identifier option?	Set to **y** to check whether the “quoted identifier” option is on. This database option controls whether double quotation mark characters (“) can be used to surround delimited identifiers. The default is n.
Read-only option?	Set to **y** to check whether the “read-only” option is on. When set, this database option specifies that database records are read-only; data cannot be modified. The default is n.
Recursive triggers option?	Set to **y** to check whether the “recursive raises” option is on. This database option enables recursive firing of raises. The default is n.
Select into/bulkcopy option?	Set to **y** to check whether the “select into/bulkcopy” option is on. When set, this database option allows unlogged database transactions. The default is n.
Single user option?	Set to **y** to check whether the “single user” option is on. When set, this database option specifies that only one user can access the database at a time. The default is n.
Subscribed option?	Set to **y** to check whether the database is configured as a subscriber database. The default is n.

Description	How to Set It
Torn page detection option?	Set to y to check whether the “torn page detection” option is on. This database option controls whether Microsoft SQL Server detects incomplete pages. The default is n.
Truncate log on chkpt option?	Set to **y** to check whether the “truncate log on chkpt” option is on. This database option controls whether the transaction log is truncated when the Checkpoint process runs. The default is n.
Event severity when option is on or off	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a selection option is on or off. The default severity level is 5 (red event indicator).

DBSpace

Use this Knowledge Script to monitor available database space and the percentage of database space being used for each database. Monitored database space includes data and log space. This script raises an event if the available database space exceeds the maximum threshold or falls below the minimum threshold you set.

You can set this script to observe new databases dynamically each time it runs. Observing databases dynamically allows you to monitor database space for databases that have been added since running the Discovery_SQL Knowledge Script and prevents you from attempting to monitor databases that have been dropped since discovery.

If you enable the *Recalculate space usage?* parameter, this script calls a Microsoft stored procedure that corrects inaccuracies in the `sysindexes` table. These inaccuracies might result in incorrect space usage reports.

Notes

- Although this script can observe new databases each time it runs, the new databases are not reflected in the Operator Console or Control Center. To gather more detailed database device information that includes space used by log devices, use the DBStats Knowledge Script.
- This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Objects

Microsoft SQL Server or Database folder, if dynamically observing databases. If you are not observing databases dynamically, you can run this script on the Database folder or individual database objects.

If you run the script on a individual database object, only that object is monitored regardless of how you set the *Dynamically observe databases at each interval?* parameter.

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe databases at each interval?	Set to **y** to dynamically observe databases at each monitoring interval. The default is y. **Note** Dynamic observation takes place only when the script is run on the Databases object, not when run on an individual database.
Exclude these objects	Specify the name of any database you want to exclude from monitoring. You can specify multiple databases, separated by commas and no spaces. For example: `master,model,mdb`. These databases are excluded even if dynamic monitoring is not enabled. You can use standard pattern-matching characters when specifying database names. • ***** matches zero or more instances of a character • **?** matches exactly one instance of a character • # matches any single digit from 0 - 9 • **[ ]** matches exactly one instance of any character between the brackets, including ranges **Note** If a database name literally matches the pattern you provide, it will be excluded. For example, if you enter `m*`, the `master`, `model`, and `msdb` databases are not monitored, nor is the database coincidentally titled `m*`.
Raise event if threshold exceeded or not met?	Set to **y** to raise an event if a monitored value exceeds or falls below the threshold. The default is y.
Raise event if database is offline?	Set to **y** to raise an event if the database is offline. The default is y.
Collect data for available and used database space?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the available database space and the percentage of database space used for each database. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the public Fixed Server Role. Also it must be in the `db_owner` Fixed Database Role for every database where you want to run this script.
Recalculate space usage?	Set to **y** to have Microsoft SQL Server recalculate the space usage. If enabled, the Knowledge Script calls a Microsoft stored procedure that corrects inaccuracies in the `sysindexes` table that might result in incorrect space usage reports. If you have a very large database, recalculating space usage will impact database performance. The default is n.
Threshold -- Minimum disk space available	Specify the minimum amount of disk space required for the database (including data space and log space) to prevent an event from being raised. If the amount of disk space falls below this threshold, an event is raised. The default is 0 MB.
Threshold -- Maximum percentage of utilized database space	Specify the maximum percentage of database space that can be used before an event is raised. The default is 90%.

Description	How to Set It
Event severity when threshold exceeded or not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored value exceeds or falls below the threshold. The default severity level is 5 (red event indicator).
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of an event for an unexpected error. The default severity level is 35.

DBStats

Use this Knowledge Script to monitor the amount of allocated space used by data and log files. Separate thresholds are available for files whose size is configured to grow automatically and for those whose size is not set to grow automatically.

If a file *is not* set to grow automatically, the percentage of used space is compared to the total space allocated for the file. This script then raises an event if the percentage of used space exceeds the threshold you specify.

If a file *is* set to grow automatically and a maximum file size is specified in Microsoft SQL Server, the percentage of used space is compared to the maximum specified size. This script then raises an event if the percentage of used space exceeds the threshold you specify.

If a file is set to grow automatically but no maximum file size is specified in Microsoft SQL Server, no event is raised.

Notes

This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

The data detail for the Log Utilization and Device Utilization graph data may show a slightly different calculated value. The difference occurs due to rounding when calculating the data and will not exceed one tenth.

The % **Of Current** value shown in the **Devices Triggering Threshold** table for the Log Utilization graph data and events is relative to all the log files and not each individual log file.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Objects

Microsoft SQL Server or Database folder, if dynamically observing databases. If you are not observing databases dynamically, you can run this script on the Database folder or on individual database objects.

If you run the script on a individual database object, only that object is monitored regardless of how you set the *Dynamically observe databases at each interval?* parameter.

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event for used data file space?	Set to **y** to raise an event if the percentage of used data file space exceeds the threshold you specify. The default is y.
Raise event for used log file space?	Set to **y** to raise an event if the percentage of used log file space exceeds the threshold you specify. The default is y.

Description	How to Set It
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the data or log file size exceeds the threshold. The default is 5 (red event indicator).
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script fails due to an error condition. The default is 5 (red event indicator).
Include values in event message?	Set to **y** to include the percentages of used file space in event messages. The default is n.
Collect data for file space usage?	Set to **y** to collect data for charts and reports. If enabled, data collection, returns the percentage of used file space for the data and log files. The default is n.
Collect data for database size?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the size of the database in MB. The default is n.
Collect data for current allocated space?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the amount of space currently allocated for a specific database. The default is n.
Collect data for current used space?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the percentage of allocated data or log file space currently in use for a specific database. The default is n.
SQL user ID	Specify the login ID used to connect to the Microsoft SQL Server managing the databases you want to monitor. Use the same login name and password specified in AppManger Security Manager. For example, if you used Security Manager to store the SQL login account `AM_OWNER` and the password for this account, then type `AM_OWNER`.
Use trusted connection?	Set to **y** to use a trusted connection rather than a SQL user ID. If you use a trusted connection, the Windows account under which the AppManager agent runs must be able to log on to the Microsoft SQL Server. The default is y.
Threshold -- Maximum used space if database file can grow	Specify the maximum percentage of used data file space allowed if the data file can grow automatically. If the percentage exceeds this amount, an event is raised. The default is 90%.
Threshold -- Maximum used space if database file cannot grow	Specify the maximum percentage of used data file space allowed if the data file cannot grow automatically. If the percentage exceeds this amount, an event is raised. The default is 75%.
Threshold -- Maximum used space if log file can grow	Specify the maximum percentage of used log file space allowed if the log file can grow automatically. If the percentage exceeds this amount, an event is raised. The default is 90%.
Threshold -- Maximum used space if log file cannot grow	Specify the maximum percentage of used log file space allowed if the log file cannot grow automatically. If the percentage exceeds this amount, an event is raised. The default is 75%.

Description	How to Set It
Dynamically observe databases at each interval?	Set to **y** to dynamically observe databases at each monitoring interval. The default is y. **Note** Dynamic observation takes place only when the script is run on the Databases object, not when it is run on an individual database.
Exclude these objects	Specify the name of any database you want to exclude from monitoring. You can specify multiple databases, separated by commas and no spaces. For example: `master,model,mdb`. These databases are excluded even if dynamic monitoring is not enabled. You can use standard pattern-matching characters when specifying database names. • ***** matches zero or more instances of a character • **?** matches exactly one instance of a character • # matches any single digit from 0 - 9 • **[ ]** matches exactly one instance of any character between the brackets, including ranges **Note** If a database name literally matches the pattern you provide, it will be excluded. For example, if you enter `m*`, the `master`, `model`, and `msdb` databases are not monitored, nor is the database coincidentally titled `m*`.

ErrorLog

Use this Knowledge Script to monitor the Microsoft SQL Server error logs (`Errorlog`, `Errorlog.*` in the Microsoft SQL Server log folder).

On the first job iteration, this script sets a starting point for future log scanning and does not scan the existing entries in the logs. Therefore it does not return any results on the first iteration. As it continues to run at the interval specified in the Schedule tab, this script scans the logs for any new entries created since the last time it checked.

This script raises an event if the number of entries that match the *Log text to match* criteria exceeds the threshold you specify.

Note
This script does not raise events or generate data points when you run it on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if new log entries found?	Set to **y** to raise an event if new log entries are found. The default is y. **Note** In general, the detail message for the Knowledge Script contains details about the occurrences found. If the message is larger than 32 KB, the data is saved in a file on the managed computer in the `\NetIQ\AppManager\bin` folder, and the detail message contains the truncated data. If you generate these log files, you should periodically remove the files when you are done with them.
Collect data for number of new log entries?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of new event log entries.The default is n.
Case-sensitive?	Set to **y** to match upper and lower case letters when checking for a match to the search string. The default is n.
Literal match?	Set to **y** if you want to search for the *entire* search string. For example, if you set this parameter to **y** and enter "`foo bar`" as the search string, only lines containing "`foo bar`" are considered a match. The default is y. Set to **n** to match *any* of the words in the *Log text to match* parameter value. For example, if you set this parameter to **n** and enter "`foo bar`" as the search string, any lines that contain "`foo`," "`bar`," or "`foo bar`" are considered a match.

Description	How to Set It
Log text to match	Specify all or part of the string you want to check for. Separate multiple search strings with commas. The default is `Wait-for graph`. **Note** The text string `Wait-for graph` can be used to catch deadlocks that might occur on the Microsoft SQL Server instance you are monitoring. However, if this string is used, the Microsoft SQL Server instance must have additional tracing enabled. For more information, see Microsoft Knowledge Base article 832524.
Text to exclude	Specify a string or series of strings of text that you want to exclude from the search results. Use semi-colons to separate multiple strings.
Threshold -- Maximum number of new log entries	Specify the maximum number of new log entries that can be matched before an event is raised. The default is 0 (the first instance exceeds the threshold and raises an event).
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of new log entries exceeds the threshold. The default severity level is 5 (red event indicator).
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of an event for an unexpected error, such as when the SQL server is not accessible, or SQL Server authentication failed. The default severity level is 35.

ErrorLogEx

Use this Knowledge Script to monitor the SQL Server error log for entries added since the last monitoring interval that match your criteria.

This script allows you to exclude log entries based on a set of specified strings, and the script allows you to treat all strings as regular expressions. Also, this script raises an event if the number of new entries exceeds the threshold you set.

On the first job iteration, this script sets a starting point for future log scanning and does not scan the existing entries in the logs. As a result, the script does not return any results on the first iteration. As the script continues to run at the interval specified in the Schedule tab, this script scans the logs for any new entries created since the last time it checked.

Note
This script does not raise events or generate data points when you run it on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if new log entries exceed threshold?	Set to **y** to raise an event if new log entries exceed the threshold you set. The default is y. **Note** In general, the detail message for the Knowledge Script contains details about the occurrences found. If the message is larger than 32 KB, the data is saved in a file on the managed computer in the `\NetIQ\AppManager\bin` folder, and the detail message contains the truncated data. If you generate these log files, you should periodically remove the files when you are done with them.
Collect data for number of new log entries?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of new event log entries.The default is n.
Enforce case-sensitivity in all strings?	Set to **y** to match upper and lower case letters when checking for a search string matches. The default is n.
Treat all strings as regular expressions?	Set to **y** if you want to use regular expressions to specify or exclude search strings. The default is n, which allows you to use a literal search instead of a search using regular expressions. Refer to the Windows `findstr` command for the syntax of regular expressions.

Description	How to Set It
Strings to find	Specify all or part of the string you want to find in the error log. If you want to include multiple search stings, separate the strings with commas, without spaces. Do not use semi-colons. **Note** Two successive commas are treated as a single literal comma. For example, the script interprets the following text as two strings: `string,,one,string_two` (string,one and string_two). Refer to the Windows `findstr` command for the syntax of regular expressions. The default is `Wait-for graph`, which you can use to catch deadlocks that might occur on the Microsoft SQL Server instance you are monitoring. However, if you use this string, the Microsoft SQL Server instance must have additional tracing enabled. For more information, see Microsoft Knowledge Base article 832524.
Strings to exclude	Specify a string or series of strings of text that you want to exclude from the search results. Use commas to separate multiple strings.
Threshold -- Maximum number of new log entries	Specify the maximum number of new log entries that can be matched before an event is raised. The default is 0, which means that the first time the script matches the search string, the script raises an event.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of new log entries exceeds the threshold. The default severity level is 5 (red event indicator).
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the job fails. The default severity level is 5 (red event indicator).

LockUtil

Use this Knowledge Script to monitor how long users must wait for lock requests to expire. This script raises an event if the waiting period for lock requests exceeds the threshold you set.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server

Default Schedule

The default schedule for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if lock request wait time exceeds threshold?	Set to **y** to raise an event if the lock request wait time exceeds the threshold. The default is y.
Collect data for lock request wait time?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about how long a user must wait for a lock request to expire. The default is n.
Threshold -- Maximum lock request wait time	Specify the maximum number of milliseconds that a user can spend waiting for a lock request to expire before an event is raised. The default is 100 ms.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the lock request wait time exceeds the threshold. The default severity level is 5 (red event indicator).

LogGrowthRate

Use this Knowledge Script to monitor log growth and shrinkage rates for all Microsoft SQL Server databases. Growth and shrinkage rates are calculated by taking the difference of the log space utilization from the current monitoring interval and the log space utilization from the previous interval. This script raises an event if either rate exceeds the threshold you set.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Objects

Microsoft SQL Server or Database folder, if dynamically observing databases. If you are not observing databases dynamically, you can run this script on the Database folder or individual database objects. If you run the script on a individual database object, only that object is monitored regardless of how you set the *Dynamically observe databases at each interval?* parameter.

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe databases at each interval?	Set to **y** to dynamically observe databases at each monitoring interval. The default is y. **Note** Dynamic observation takes place only when the script is run on the Databases object, not when it is run on an individual database.
Exclude these objects	Specify the name of any database you want to exclude from monitoring. You can specify multiple databases, separated by commas and no spaces. For example: `master,model,mdb`. These databases are excluded even if dynamic monitoring is not enabled. You can use standard pattern-matching characters when specifying database names. • ***** matches zero or more instances of a character • **?** matches exactly one instance of a character • # matches any single digit from 0 - 9 • **[ ]** matches exactly one instance of any character between the brackets, including ranges **Note** If a database name literally matches the pattern you provide, it will be excluded. For example, if you enter `m*`, the `master`, `model`, and `msdb` databases are not monitored, nor is the database coincidentally titled `m*`.

Description	How to Set It
Raise event if threshold exceeded or not met?	Set to **y** to raise an event if a monitored value exceeds or falls below the threshold. The default is y.
Raise event if database is offline?	Set to **y** to raise an event if the database is offline. The default is y.
Collect data for log growth and shrinkage rates?	Set to **y** to collect data for charts and reports. If enabled, data collection, returns the log growth and shrinkage rates for each database. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "sa" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the public Fixed Server Role. Also it must be in the db_owner Fixed Database Role for every database where you want to run this job.
Threshold -- Maximum log growth rate	Specify the maximum log growth rate, as a percentage, that is allowed between the last and current interval before an event is raised. The default is 25%.
Threshold -- Maximum log shrinkage rate	Enter the maximum log shrinkage rate, as a percentage, that is allowed between the last and current interval before an event is raised. The default is 25%.
Event severity when threshold exceeded or not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored value exceeds or falls below the threshold. The default severity level is 5 (red event indicator).

LoginFailures

Use this Knowledge Script to monitor Microsoft SQL Server login failures. You can use this information to check for unauthorized attempts to access SQL Server and also to monitor login failure of specific login names.

You can specify the maximum number of failed logins to be displayed and specify whether data needs to be collected for creating charts and reports. You can also specify the maximum number of rows of failed login information to be written to a file, which you can view later.

This script raises an event if SQL login fails or if the script is run on a version of SQL Server earlier than version 2005.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2005 and 2008

Resource Objects

Microsoft SQL Server and database levels

Default Schedule

The default interval for this script is **Asynchronous**. All other schedule types are unavailable.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Event severity when login fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a login to SQL Server fails. The default event severity level is 15.
Event Detail Options	
Maximum number of failed logins to display	Specify the maximum number of failed logins to display in an event message. The default is 10 logins.
Data Collection	
Collect data for top login failures?	Set to **Yes** to collect data about top login failures data for charts and reports. By default, data collection is disabled.
Data Detail Options	
Number of rows to display in data details	Specify the maximum number of rows of data details to be displayed. The default is 10 rows.
Monitoring	

Description	How to Set It
Microsoft SQL Server login	Specify the Microsoft SQL Server user name needed to access the Microsoft SQL Servers. This login must have permission to access the servers on which you want to monitor login failure. If you do not enter the Microsoft SQL Server login, AppManager uses Windows authentication.
Comma-separated user names to monitor	Specify the specific Microsoft SQL Server user names to monitor, using commas as separators. AppManager runs the Knowledge Script and displays the filtered results based on the specific user names you enter.
Save top failed login user information to a file?	Select the **Yes** check box to save login failure information to a file. By default, saving login information is disabled.
Full path to the file	Specify the full path to the file where you want to save the login failure information.
File Content Options	
User information to write to file	Specify the maximum number of rows of failed login information to be written to the file. The information includes the login name and the number of times that login fails. The default is 10 rows.

LogShipping

Use this Knowledge Script to monitor log shipping metrics. Log shipping is a process in which transaction logs from a primary Microsoft SQL Server are applied sequentially on a scheduled basis to another Microsoft SQL Server.

On the first job iteration, this script sets a starting point for future log scanning and does not scan the existing entries in the logs. Therefore, it does not return any results on the first iteration. As it continues to run at the interval specified in the Schedule tab, this script scans the logs for any new entries created since the last time it checked.

This script raises an event if the number of successful log shipping records exceeds the threshold you specify, and if log shipping fails for any reason.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Objects

Microsoft SQL Server instances

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if log shipping fails?	Set to **Yes** to raise an event if log shipping fails. The default is Yes.
Event severity when log shipping fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which log shipping fails. The default severity level is 5.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event if the number of successful log shipping records exceeds threshold. The default is Yes.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of successful log shipping records exceeds the threshold. The default severity level is 15.
Data Collection	
Collect data for log shipping?	Set to **Yes** to collect log shipping data for charts and reports. The default is Yes.
Custom data stream legend	Specify a custom data stream legend to display in the **Graph Data** tab.

Description	How to Set It
Monitoring	
Threshold - Maximum number of successful log shipping records	Specify the maximum number of successful log shipping records that can be found before an event is raised. The default number of records is 100.

LogSpace

Use this Knowledge Script to monitor a database's available log space and track log space usage. This script raises an event if the available log space falls below the threshold you set, or if the percentage of log space used exceeds the threshold you set.

You can set this script to observe new databases dynamically each time it runs. Observing databases dynamically allows you to monitor log space for databases that have been added since you ran the Discovery_SQL Knowledge Script and prevents you from attempting to monitor databases that have been dropped since discovery.

Notes

- Although this script can observe new databases each time it runs, the new databases are not reflected in the Operator Console or Control Center.
- This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Objects

Microsoft SQL Server or Database folder, if dynamically observing databases. If you are not observing databases dynamically, you can run this script on the Database folder or individual database objects. If you run the script on a individual database object, only that object is monitored regardless of how you set the *Dynamically observe databases at each interval?* parameter.

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe databases at each interval?	Set to **y** to dynamically observe databases at each monitoring interval. The default is y. **Note** Dynamic observation takes place only when the script is run on the Databases object, not when it is run on an individual database.
Exclude these objects	Specify the name of any database you want to exclude from monitoring. You can specify multiple databases, separated by commas and no spaces. For example: `master,model,mdb`. These databases are excluded even if dynamic monitoring is not enabled. You can use standard pattern-matching characters when specifying database names. • ***** matches zero or more instances of a character • **?** matches exactly one instance of a character • # matches any single digit from 0 - 9 • **[ ]** matches exactly one instance of any character between the brackets, including ranges **Note** If a database name literally matches the pattern you provide, it will be excluded. For example, if you enter `m*`, the `master`, `model`, and `msdb` databases are not monitored, nor is the database coincidentally titled `m*`.
Raise event if threshold exceeded or not met?	Set to **y** to raise an event if a monitored value exceeds or falls below the threshold. The default is y.
Raise event if database is offline?	Set to **y** to raise an event if the database is offline. The default is y.
Collect data for space available and space used?	Set to **y** to collect data for charts and reports. If enabled, data collection, returns the available log space and the percentage of log space used for each database. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the public Fixed Server Role. Also it must be in the `db_owner` Fixed Database Role for every database where you want to run this job.
Threshold -- Minimum disk space available	Specify the minimum disk space required for the database's log space. If the amount of disk space falls below this threshold, an event is raised.The default is 0 MB.
Threshold -- Maximum percentage of log space used	Specify the maximum percentage of log space that can be used before an event is raised. The default is 90%.
Event severity when threshold exceeded or not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored value exceeds or falls below the threshold. The default severity level is 5 (red event indicator).

MemUtil

Use this Knowledge Script to monitor the amount of memory used by Microsoft SQL Server processes: `sqlservr`, `sqlagent`, and `sqlexec`. This script raises an event if memory usage exceeds the maximum threshold you set, and if the number of free pages falls below the minimum threshold you set.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server

Default Schedule

The default schedule for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold exceeded or not met	Set to **y** to raise an event if a monitored value exceeds or falls below the threshold. The default is y.
Collect data for memory usage and free pages?	Set to **y** to collect data for charts and reports. If enabled, data collection returns total server memory in MB, the number of free pages, and the working set, in MB, of each associated SQL Server process. The default is n.
Threshold -- Maximum memory usage	Specify the maximum amount of memory that can be consumed by Microsoft SQL Server processes before an event is raised. The default is 75 MB.
Threshold -- Minimum number of free pages	Specify the minimum number of pages that must be free to prevent an event from being raised. The default is 50 pages.
Threshold -- Maximum server memory usage	Specify the maximum amount of memory that can be consumed by Microsoft SQL Server and all related processes before an event is raised. The default is 3000 MB.
Event severity when threshold exceeded or not met	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored value exceeds or falls below the threshold. The default severity level is 5 (red event indicator).

MonitorDDL

Use this Knowledge Script to monitor Data Definition Language (DDL) statements. DDL statements are executed by database administrators during the setup and modification of database schema. Any change in schema results in a change in the data model and therefore monitoring such changes on a production server is crucial.

This script raises an event when a DDL execution takes place. You can then determine whether the change is authorized by a competent authority.

Notes
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

If you move a cluster group in Cluster Administrator:

- Stop the MonitorDDL Knowledge Script running on the clustered nodes.
- Delete the `logddlstatements` trigger and `ddl_log` table from the monitored database.
- Run a new job on the clustered nodes.

Version Compatibility

Microsoft SQL Server 2005 and 2008

Resource Objects

Microsoft SQL Server instances

Default Schedule

The default interval for this script is **Asynchronous**. All other schedule types are unavailable.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Event Detail Options	
Include DDL executed statements in event details?	Set to **Yes** to allow events to contain DDL statements in an event message. If set to Yes, a DDL Statement column is displayed in the detailed event message. By default, including DDL statements in the event details is enabled.
Number of executed DDL statements to display	Specify the maximum number of executed DDL statements to display in the event message. This number must be between 1 and 1000. The default is 10 statements.
Data Collection	
Collect data for DDL statements executed?	Set to **Yes** to collect DDL statements data for charts and reports. By default, data is disabled.
Data Detail Options	

Description	How to Set It
Include DDL statements in the data details?	Set to **Yes** to display data details in a table. The data consists of: • Time: Statement execution time. • Microsoft SQL Server: Microsoft SQL Server name. • Database Name: Database name on which query is executed. • User Name: Name of the user executing the query. • DDL Statement: Executed DDL statement. By default, including DDL statements in the data details is disabled.
Number of statements to display in data details	Specify the maximum number of rows to display in the data details. This number must be between 1 and 1000. The default is 10 rows.
Monitoring	
Microsoft SQL Server login	Specify the secondary database user login account needed to access Microsoft SQL Server. The user name you enter must have the permission to access the databases on which you want to monitor DDL statements.
Database to be monitored	Specify the name of the database on which to monitor the DDL statements. This is a mandatory field.
Save executed DDL statements to a file?	Set to **Yes** to save executed DDL statements to a file. By default, saving executed DDL statements is disabled.
Full path to file	Specify the full path to the file that contains the executed DDL statements information.
File Content Options	
Number of rows to write to the file	Specify the maximum number of rows to write to the file. This number must be between 1 and 1000. The default number is 10.
Append to the file?	Set to **Yes** to append new rows to the existing rows in the file. Not setting to Yes clears the data from the file before storing new rows. By default, appending to the file is disabled.

MonitorJobs

Use this Knowledge Script to query Microsoft SQL Server and report on any jobs that have not successfully completed. If a job fails, an event contains the following message: `N SQL jobs failed on ServerName`. In addition, if the number of failed jobs exceeds the threshold you specify, an event is raised. By default, this script raises events only when new job failures occur since the last monitoring interval. You can specify the jobs to monitor.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Required SQL Permissions

This Knowledge Script requires a SQL Server user login account that has Select access to the `sysjobs` and `sysjobservers` tables.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
SQL login	Specify the database user login account that will run the SQL statements. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** In general, permission to run specific SQL commands and statements is derived from the permissions granted to the login account you are using to run this Knowledge Script. However, the `dbcc` command can only be run by: • `dbo` account (Microsoft SQL Server 2000, 2005, and 2008) • `db_backupoperator` account (Microsoft SQL Server 2000, 2005, and 2008)
Collect data for number of failed jobs?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the number of jobs that have failed, including the job name and the reason for the failure. The default is Yes.
Raise event if job failures exceed threshold?	Set to **Yes** to raise an event if the number of job failures exceeds the threshold. The default is Yes.

Description	How to Set It
Threshold -- Maximum number of failed jobs	Specify the maximum number of failed jobs that can be detected before an event is raised. The default is 0 jobs.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of failed jobs exceeds the threshold. The default severity level is 5 (red event indicator).
Only event when new job failures occur?	Set to **Yes** to raise events for failed jobs *only* when failures have occurred since the last monitoring interval. When this option is selected, an event is not raised on previously failed jobs until a new failure is detected. By default, events are raised if the time of the job error is later than the last monitoring interval.
Only event on these jobs	Specify the names of jobs to include in monitoring. Separate multiple names with a comma. Only specified job names are included in data collection and have events raised if job failures are detected. By default, all jobs are monitored.
Event severity for unexpected error	Set the event severity level, from 1 to 40, to indicate the importance of an event for an unexpected error, such as when the SQL server is not accessible, or SQL Server authentication failed. The default severity level is 35.

NearFileMaxSize

Use this Knowledge Script to monitor the size of Microsoft SQL Server database files. You can set a threshold to determine when a file is reaching its maximum size. Thresholds are available for a maximum file size and for a maximum percentage of the allowed file size that a database file can reach. This script raises an event if the size of any database file exceeds a threshold you set.

You can set this script to observe new databases dynamically each time it runs. Observing databases dynamically allows you to monitor file size for databases that have been added since running the Discovery_SQL Knowledge Script and prevents you from attempting to monitor databases that have been dropped since discovery.

Notes

- Although this script observes new databases each time it runs, the new databases are not reflected in the Operator Console or Control Center.
- This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Objects

Microsoft SQL Server or Database folder, if dynamically observing databases. If you are not observing databases dynamically, you can run this script on the Database folder or individual database objects. If you run the script on a individual database object, only that object is monitored regardless of how you set the *Dynamically observe databases at each interval?* parameter.

Default Schedule

The default interval for this script is **Once every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Dynamically observe databases at each interval?	Set to **y** to dynamically observe databases at each monitoring interval. The default is y. **Note** Dynamic observation takes place only when the script is run on the Databases object, not when it is run on an individual database.
Exclude these objects	Specify the name of any database you want to exclude from monitoring. You can specify multiple databases, separated by commas and no spaces. For example: `master,model,mdb`. These databases are excluded even if dynamic monitoring is not enabled. You can use standard pattern-matching characters when specifying database names. • ***** matches zero or more instances of a character • **?** matches exactly one instance of a character • # matches any single digit from 0 - 9 • **[ ]** matches exactly one instance of any character between the brackets, including ranges **Note** If a database name literally matches the pattern you provide, it will be excluded. For example, if you enter `m*`, the `master`, `model`, and `msdb` databases are not monitored, nor is the database coincidentally titled `m*`.
Raise event if file size exceeds threshold?	Set to **y** to raise an event if database file size exceeds the threshold. The default is y.
Raise event if database is offline?	Set to **y** to raise an event if the database is offline. The default is y.
Collect data for database file size?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the size of the database files.The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the public Fixed Server Role. Also it must be in the `db_owner` Fixed Database Role for every database where you want to run this job.
Threshold -- Maximum database file size	Specify the maximum file size that database files can reach before an event is raised. The default is 500 MB.
Threshold -- Maximum percentage of allowed size	Specify the maximum percentage of its maximum allowed size that a file can use before an event is raised. The default is 90%.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which database file size exceeds the threshold. The default severity level is 5 (red event indicator).

NearMaxConnect

Use this Knowledge Script to monitor the opened connection usage of Microsoft SQL Server. This script compares the current number of connections being used to the maximum number of connections configured for the server. This script raises an event if the used percentage (current connections or maximum connections) exceeds the threshold you set.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

If the user connection configuration variable is a value, you can run this script on Microsoft SQL Server 2000, 2005, and 2008 to monitor user connections. If you are using Microsoft SQL Server 2000, 2005, or 2008 and have not set the maximum user connections (that is, you let Microsoft SQL Server configure the maximum number of user connections on its own), then you cannot use this script to collect data. A value of 0 is always returned.

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if used connections exceed threshold?	Set to **y** to raise an event if the percentage of used connections exceeds the threshold. The default is y.
Collect data for number of connections used?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the number of open connections being used. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "sa" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the public Fixed Server Role. Also it must be in the `db_owner` Fixed Database Role for every database where you want to run this job.
Threshold -- Maximum percentage of connections used	Specify the maximum percentage of connections that can be in use before an event is raised. The default is 95%.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of used connections exceeds the threshold. The default severity level is 5 (red event indicator).

NearMaxLocks

Use this Knowledge Script to monitor the lock usage of Microsoft SQL Server. This script compares the current number of locks being used to the maximum number of locks configured for the server. This script raises an event if the used percentage of current locks or maximum locks exceeds the threshold you set.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

If you have set the lock configuration variable to a value, you can run this script on Microsoft SQL Server 2000, 2005, and 2008 to monitor lock usage. You cannot use this script to collect data for SQL Server 2000, 2005, or 2008 if you have not set the maximum number of locks. In other words, you let SQL Server configure the maximum number of locks for you, in which case a value of 0 is always returned.

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if percentage of used locks exceeds threshold?	Set to **y** to raise an event if the percentage of used locks exceeds the threshold. The default is y.
Collect data for percentage of used locks?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the percentage of locks being used. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the public Fixed Server Role. Also it must be in the `db_owner` Fixed Database Role for every database where you want to run this job.
Threshold --Maximum percentage of locks utilized	Specify the maximum percentage of locks that can be in use before an event is raised. The default is 95%.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of used locks exceeds the threshold. The default severity level is 5 (red event indicator).

NetError

Use this Knowledge Script to monitor Microsoft SQL Server network errors. This script compares the number of packet errors that occurred between the current and previous monitoring intervals. This script raises an event if the number of errors exceeds the threshold you set. In addition, this script generates data streams for the number of network errors.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if network errors exceed threshold?	Set to **y** to raise an event if the number of network errors exceeds the threshold. The default is y.
Collect data for number of network errors?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of network errors. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. The account must be in the public Fixed Server Role and you must explicitly grant the "`Select`" privilege on the master database.
Threshold -- Maximum number of network errors	Specify the maximum number of network errors allowed before an event is raised. The default is 0 errors.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of network errors exceeds the threshold. The default severity level is 5 (red event indicator).

ParseErrors

Use this Knowledge Script to monitor all Microsoft SQL Server parse error messages. Parse errors are Microsoft SQL Server messages that are displayed in case of any errors or exceptions. Hackers use the SQL injection technique to try and bypass the security controls of a database application. Failed attempts usually result in SQL parse errors. Using this script, you can monitor and prevent SQL injection attacks.

In addition, this script raises an event if a parse error occurs on Microsoft SQL Server.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2005 and 2008

Resource Object

Microsoft SQL Server

Default Schedule

The default interval for this script is **Asynchronous**. All other schedule types are unavailable.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if parse errors are found?	Set to **Yes** to raise an event if parse errors occur. The default is Yes.
Event severity when parse errors are found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which pars errors are found. The default severity level is 5.
Event Detail Options	
Number of rows to display	Specify the maximum number of parse error detail rows to be displayed in the event message. This number must be between 0 and 5000. The default number is 10.
Data Collection	
Collect data for number of parse errors?	Set to **Yes** to collect parse error data for charts and reports. Data details are shown as a table in the data details dialog box. The following columns are shown in the data details dialog box: • Row • ParseError By default, collection of parse errors data is disabled.

Description	How to Set It
Monitoring	
Microsoft SQL Server login	Specify the Microsoft SQL Server user login needed to access the SQL Servers. This login must have the permission to access the servers on which you want to monitor parse errors. If you do not enter the Microsoft SQL Server login, AppManager uses Windows authentication.

ProcessingTime

Use this Knowledge Script to monitor the processing time of any T-SQL statements or stored procedures. You can enter the T-SQL statements to be executed when you run this script, or you can load the statements from a script file. Use the system administrator role or `dbo` account where necessary;. For example, use `dbo` for running Database Console Commands (DBCC).

This script raises an event if the processing time for any T-SQL statement or stored procedure exceeds the threshold you set. If an index is used in the query, the results contain details of the index.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server

Default Schedule

The default schedule for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if processing time exceeds threshold?	Set to **y** to raise an event if the amount of processing time exceeds the threshold. The default is y.
Collect data for processing time?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the amount of processing time used by T-SQL statements or stored procedures. The default is y.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account needs to have sufficient privileges to run the specified command.
Load SQL statements from file?	Set to **y** to load SQL statements from a file. The default is n.
Full path to SQL script file	If you enabled *Load SQL statements from file?*, specify the complete file path for the script file containing SQL statements to execute. For example, enter `F:\NetIQ Corporation\Sample.sql` You cannot enter a path in the form of `\\computer\dir\Sample.sql` if the NetIQ Corporation Client Resource Monitor service (`netiqmc`) is running as a system account.

Description	How to Set It
SQL statement to execute	Specify the SQL statement to be executed. The default is `sp_who`. **Note** Unless you are entering very simple queries, you might find typing SQL statements into this field is error-prone. To avoid this, use the *Load SQL statements from file?* parameter. Or, if you have an AppManager Developer's license, you can check this Knowledge Script out of the repository, use the Knowledge Script Editor to paste the desired SQL statements into the SQL statement field, and then check the modified Knowledge Script back in.
Legend for output	Specify a legend for the output of your SQL Server statement. The default is blank. If left blank, AppManager constructs a legend based on the column number. For example, if the Column Number is 0, the constructed legend is "# Result Rows". If the Column Number is greater than 0, the constructed legend is the specified column heading. If no heading exists, the constructed legend is: "`Column <num> Value`"
Threshold -- Maximum processing time	Specify the maximum amount of time that T-SQL statements or stored procedures have to respond before an event is raised. The default is 10 seconds.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of processing time exceeds the threshold. The default severity level is 5 (red event indicator).

RepLatency

Use this Knowledge Script to monitor replication latency in milliseconds. This script raises an event if replication latency exceeds the threshold you set. In addition, this script generates data streams for replication latency.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwnerKnowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if latency exceeds threshold?	Set to **y** to raise an event if replication latency exceeds the threshold you set. The default is y.
Collect data for replication latency?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about replication latency. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "sa" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account needs to have sufficient privileges to run the specified command.
Threshold -- Maximum replication latency	Specify the maximum amount of replication latency allowed before an event is raised. The default is 20000 milliseconds.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which replication latency exceeds the threshold. The default severity level is 5 (red event indicator).

Replication

Use this Knowledge Script to monitor replication latency in milliseconds, the number of transactions in the transaction log of the publication database that are marked for replication but have not yet been replicated, and the number of transactions being replicated per second. It also monitors the replication agent to check whether it is running.

This script consolidates functionality that is also available in three separate SQL Knowledge Scripts: RepLatency, RepTransactions, and RepTranSec. Changes to the individual script do not affect the functionality of the consolidated script.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Required SQL Permissions

This Knowledge Script requires a SQL Server user login account that is in the public Fixed Server Role and the `sysadmin` Role.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Replication Latency	Set to **Yes** to check for replication latency. By default, replication latency is disabled.
Raise event if latency exceeds threshold?	Set to **Yes** to raise an event if replication latency exceeds the threshold you set. The default is Yes.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which replication latency exceeds the threshold. The default severity level is 5.
Collect data for replication latency?	Set to **Yes** to collect replication latency data for charts and reports. By default, data collection is disabled.
Threshold - Maximum replication latency	Specify the maximum amount of replication latency allowed before an event is raised. The default is 20000 milliseconds.
Pending Replication Transaction	Set to **Yes** to check for any pending replication transaction. By default, pending replication transaction is enabled.

Description	How to Set It
Raise event if pending replications exceed threshold?	Set to **Yes** to raise an event if the number of pending replications exceeds threshold. The default is Yes.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the an event in which the number of pending replication transactions exceeds the threshold. The default severity level is 5.
Collect data for number of pending replications?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the number of transactions in the transaction log marked for replication. By default, data collection is disabled.
Threshold -- Maximum number of pending replication transactions	Specify the maximum number of transactions that can be replicated in the publication database before an event is raised. The default is 1000 pending replications.
Replication Rate	Set to **Yes** to check for replication rate. By default, checking replication rate is enabled.
Raise event if replication rate exceeds threshold?	Set to **Yes** to raise an event if the replication rate exceeds the threshold you set. The default is Yes.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the replication rate exceeds the threshold. The default severity level is 5.
Collect data for replication rate?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the number of transactions being replicated per second. By default, data collection is disabled.
Threshold -- Maximum replication rate	Specify the maximum number of transactions that can be replicated per second before an event is raised. The default is 1000 transactions per second.
Replication Agent	Set to **Yes** to run the replication agent. By default, replication agent is disabled.
Raise event if replication agent is not running?	Set to **Yes** to raise an event if the replication agent is not running. The default is Yes.
Event severity when agent is not running	Set the event severity level, from 1 to 40, to indicate the importance of the an event in which the replication agent is not running. The default severity level is 5.
Collect data for agent running?	Set to **Yes** to collect data for charts and reports. By default, data collection is disabled.
Threshold -- Maximum agent running	Specify the maximum number of agents that can be running before an event is raised. The default is 10 agents.
Monitor	
Microsoft SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. The user name you enter must have the permission to access the databases on which you want to monitor replication.

Report_Accessibility

Use this Knowledge Script to generate a report about the accessibility of Microsoft SQL Servers and databases. This report uses data collected by the Accessibility Knowledge Script.

Note
The Accessibility Knowledge Script incorrectly equates stopping a job with stopping the server on which the job is running, and thus returns incorrect values for server uptime or downtime. For example, you run a job with the Accessibility Knowledge Script for two hours and then for some reason, stop the job (but not the server). You restart the job again three hours later, and it runs for an additional two hours. Although the server was running continuously for seven hours, the report will show the server downtime as three hours and server uptime as four hours.

Resource Object

Report agent

Default Schedule

The default schedule for this script is **Run once**. You should run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Data settings	
Hours or percentage on chart	Select whether to illustrate availability by hours or by percentage.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top *N*% of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N*% of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Report settings	

Description	How to Set It
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_CacheHitRatio

Use this Knowledge Script to generate a report about the percentage of time requested pages are found in the Microsoft SQL Server data cache. This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the CacheHitRatio Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers. Each page shows all the data streams collected from a single computer. • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers. Each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer. • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_DatabaseDataSpace

Use this Knowledge Script to generate a report about the data space available in MB and the percentage of data space being used in SQL databases. This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the DataSpace Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_DataSpaceAvailabilitySummary

Use this Knowledge Script to generate a report about the data space available in MB in SQL databases. This script allows you to develop a statistical summary of the data you select, for example, the average value of data points over the period you define for the report.

This report uses data collected by the DataSpace Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend. The legend is a truncated form of the data stream legend visible in the Operator Console. • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top *N*% of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N*% of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_DataSpaceUtilizationSummary

Use this Knowledge Script to generate a report about the percentage of data space used in SQL databases. This script allows you to develop a statistical summary of the data you select, for example, the average value of data points over the period you define for the report.

This report uses data collected by the DataSpace Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top *N*% of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N*% of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_DBSpaceAvailabilitySummary

Use this Knowledge Script to generate a report about the database space available in MB in SQL databases. This script allows you to develop a statistical summary of the data you select, for example, the average value of data points over the period you define for the report.

This report uses data collected by the DBSpace Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top *N*% of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N*% of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_DBSpaceAvailable

Use this Knowledge Script to generate a report about the database space available in MB and the percentage of database space used in SQL databases. This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the DBSpace Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_DBSpaceUtilizationSummary

Use this Knowledge Script to generate a report about the percentage of database space used in SQL databases. This script allows you to develop a statistical summary of the data you select, for example, the average value of data points over the period you define for the report.

This report uses data collected by the DBSpace Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top *N*% of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N*% of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ErrorLogSummary

Use this Knowledge Script to generate a report about entries in the Microsoft SQL Server error logs. This script allows you to develop a statistical summary of the data you select, for example, the average value of data points over the period you define for the report.

This report uses data collected by the ErrorLog Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top *N*% of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N*% of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_NearMaxConnect

Use this Knowledge Script to generate a report about the number of open connections to Microsoft SQL Servers versus the number of allowable connections. This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the NearMaxConnect Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_NearMaxLocks

Use this Knowledge Script to generate a report about the number of used locks to Microsoft SQL Servers versus the number of allowable locks. This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the NearMaxLocks Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_NetError

Use this Knowledge Script to generate a report about the number of packet errors. This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the NetError Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse** to select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_Replication

Use this Knowledge Script to generate a report about replication latency on your Microsoft SQL Servers, the number of transactions in the transaction log marked for replication, the number of transactions replicated per second by Microsoft SQL Servers, and replication agent details. This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the Replication Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Replication Type	Set to **yes** to create a Replication Type report. By default, report creation is disabled.
Replication Latency report	Set to **yes** to create a Replication Latency report. By default, report creation is disabled.
Transaction Replicated Per Second Report	Set to **yes** to create a Transaction Replicated Per Second report. By default, report creation is disabled.
To Be Replicated Transaction Report	Set to **yes** to create a To Be Replicated Transaction report. By default, report creation is disabled.
Agent Running Report	Set to **yes** to create an Agent Running report. By default, report creation is disabled.
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.

Description	How to Set It
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This helps make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ReplicationLatency

Use this Knowledge Script to generate a report about replication latency on your Microsoft SQL Servers. This report lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the RepLatency Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_SpaceAvailability

Use this Knowledge Script to generate a report about the data space and database space available in MB, and the percentage of data space and database space used in SQL databases.

This script consolidates functionality also available from two separate SQL Knowledge Scripts: Report_DatabaseDataSpace and Report_DBSpaceAvailable. Changes made to the individual scripts do not affect the functionality of this consolidated script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Database Report	
Database Data Space Report	Set to **yes** to generate the Database Data Space report. The default is no.
DB Space Availability Report	Set to **yes** to generate the DB Space Availability report. The default is no.
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select database data space properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_SpaceAvailabilitySummary

Use this Knowledge Script to generate a summary report about the data space and database space available in MB in SQL databases.

This script consolidates functionality also available from two separate Knowledge Scripts: Report_DataSpaceAvailabilitySummary and Report_DBSpaceAvailabilitySummary. Changes to the individual scripts do not affect the functionality of this consolidated script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. You should run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Database Report	
Data Space Availability Summary Report	Set to **yes** if you want to generate the Data Space Availability Summary report. The default is no.
DB Space Availability Summary Report	Set to **yes** if you want to generate the DB Space Availability Summary report. The default is no.
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you select • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console) • **By computer and legend** shows one value for each unique legend from each computer
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report
Select sorting/display option	Select the sorting order for data, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top *N*% of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N*% of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This helps make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.

Description	How to Set It
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_SpaceUtilizationSummary

Use this Knowledge Script to generate a summary report about the percentage of data space and database space used in SQL databases.

This script consolidates functionality also available from two separate SQL Knowledge Scripts: Report_DataSpaceUtilizationSummary and Report_DBSpaceUtilizationSummary. Changes made to the individual scripts do not affect the functionality of this consolidated script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Database Report	
Data Space Utilization Summary Report	Set to **yes** to generate the Data Space Utilization Summary report. The default is no.
DB Space Utilization Summary Report	Set to **yes** to generate the DB Space Utilization Summary report. The default is no.
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you select • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console) • **By computer and legend** shows one value for each unique legend from each computer
Data settings	

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report
Select sorting/display option	Select the sorting order for data, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top *N*% of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N*% of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.

Description	How to Set It
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_To-Be-ReplicatedTransactions

Use this Knowledge Script to generate a report about the number of transactions in the transaction log of the publication database that are marked for replication but not yet replicated. This report lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the RepTransactions Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopCPUUsers

Use this Knowledge Script to generate a report about the total CPU time (in milliseconds) used by SQL users and their connections. This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the TopCPUUsers Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopCPUUsersDetail

Use this Knowledge Script to generate a detailed report about each data point collected by the TopCPUUsers script during the time range you specify. Details include:

- Computer name
- Data stream name
- Time at which the data point was collected
- The user name
- The number of milliseconds of CPU time for that user

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopIOUsers

Use this Knowledge Script to generate a report about the number of I/O read and write operations by SQL users and their connections. This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the TopIOUsers Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopIOUsersDetail

Use this Knowledge Script to generate a detailed report about each data point collected by the TopIOUsers script during the time range you specify. Details include:

- Computer name
- Data stream name
- Time at which the data point was collected
- The user name
- The cumulative number of I/O operations for that user

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopLockUsers

Use this Knowledge Script to generate a report about the number of locks held by SQL users and their connections. This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the TopLockUsers Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopLockUsersDetail

Use this Knowledge Script to generate a detailed report about each data point collected by the TopLockUsers script during the time range you specify. Details include:

- Computer name
- Data stream name
- Time at which the data point was collected
- The user name
- The number of locks held by that user

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopMemoryUsers

Use this Knowledge Script to generate a report about the memory (by number of 8-KB pages) that can be allocated to SQL users and their connections. This report lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the TopMemoryUsers Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopMemoryUsersDetail

Use this Knowledge Script to generate a detailed report about each data point collected by the TopMemoryUsers script during the time range you specify. Details include:

- Computer name
- Data stream name
- Time at which the data point was collected
- The user name
- The number of memory pages allocated to that user

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	

Description	How to Set It
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopResourceUsers

Use this Knowledge Script to generate a report on the total CPU time (in milliseconds) used by SQL users and their connections, the number of I/O read and write operations by SQL users and their connections, number of locks held by SQL users and their connections, and the memory (by number of 8-KB pages) that can be allocated to SQL users and their connections.

This script consolidates functionality also available from four separate Knowledge Scripts: Report_TopCPUUsers, Report_TopIOUsers, Report_TopLockUsers and Report_TopMemoryUsers. Changes to the individual scripts do not affect the functionality of this consolidated script.

This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the TopResourceUsers Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day

Description	How to Set It
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.
Statistics to show per period	Select a statistical method to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This helps make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TransactionsReplicatedPerSec

Use this Knowledge Script to generate a report about the number of transactions replicated per second by Microsoft SQL Servers. This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the RepTranSec Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_UserConnections

Use this Knowledge Script to generate a report about the number of Microsoft SQL Server user connections. This script lets you aggregate data by period (minute, hour, or day) and calculate statistics for each period. For example, the average value per hour.

This report uses data collected by the UserConnections Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_UserConnectionsSummary

Use this Knowledge Script to generate a report about the number of Microsoft SQL Server user connections. This script allows you to develop a statistical summary of the data you select, for example, the average value of data points over the period you define for the report.

This report uses data collected by the UserConnections Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the period covered by the report • **Minimum**: The minimum value of data points for the period covered by the report • **Maximum**: The maximum value of data points for the period covered by the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the period covered by the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **Standard Deviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the period covered by the report • **Close**: The last value for the period covered by the report • **Change**: The difference between the first and last values for the period covered by the report (close - open = change) • **Count**: The number of data points for the period covered by the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value. Lowest to highest from front to back; highest to lowest from left to right. • **Top %**: Chart only the top *N*% of selected data (sorted by default) • **Top N**: Chart only the top *N* of selected data (sorted by default) • **Bottom %**: Chart only the bottom *N*% of data (sorted by default) • **Bottom N**: Chart only the bottom *N* of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percent or count defined in the previous parameter. For example, Top 10%, or Top 10. The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom *N* or %. For example, only the top 10%. Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_UserMaxConnections

Use this Knowledge Script to generate a report on the number of open connections to Microsoft SQL Servers versus the number of allowable connections, and the number of Microsoft SQL Server user connections.

This script consolidates functionality also available from two separate Knowledge Scripts: Report_NearMaxConnect and Report_UserConnections. Changes made to the individual scripts do not affect the functionality of this consolidated script.

This report uses data collected by the UserMaxConnection Knowledge Script.

Resource Objects

Report agent

Default Schedule

The default schedule is **Run once**. Run the report script every 30 minutes for optimal report generation.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
Select time range	Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Select the days of the week to include in your report.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval. For example, the average value for 1 Hour. • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Include table?	Set to **yes** to include a table of data stream values in the report. The default is yes.
Include chart?	Set to **yes** to include a chart of data stream values in the report. The default is yes.
Select chart style	Define the graphic properties of the charts in your report.
Select output folder	Set options for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default is no.
Select properties	Set miscellaneous report properties as needed.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the generated report contains no data. The default is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

RepTransactions

Use this Knowledge Script to monitor the number of transactions in the transaction log of the publication database that are marked for replication but have not yet been replicated. This script raises an event if the number is higher than the threshold you set. In addition, this script generates data streams for the number of pending replications.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwnerKnowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if pending replications exceed threshold?	Set to **y** to raise an event if the number of pending replications exceeds the threshold you set. The default is y.
Collect data for number of pending replications?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of transactions in the transaction log marked for replication. The default is n.
Threshold -- Maximum number of pending replication transactions	Specify the maximum number of transactions that can be replicated in the publication database before an event is raised. The default is 1000 pending replications.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of pending replications exceeds the threshold. The default severity level is 5 (red event indicator).

RepTranSec

Use this Knowledge Script to monitor the number of transactions being replicated per second. This script raises an event if the replication rate exceeds the threshold you set. In addition, this script generates data streams for the number of transactions replicated per second.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if replication rate exceeds threshold?	Set to **y** to raise an event if the replication rate exceeds the threshold you set. The default is y.
Collect data for replication rate?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of transactions being replicated per second. The default is n.
Threshold -- Maximum replication rate	Specify the maximum number of transactions that can be replicated per second before an event is raised. The default is 1000 transactions per second.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the replication rate exceeds the threshold. The default severity level is 5 (red event indicator).

RunSql

Use this Knowledge Script to run SQL statements or stored procedures. You can enter the SQL Server statements to be executed when you run this script, or you can load the statements from a script file and specify a full path to the file you want to use.

You can set maximum and minimum thresholds to be compared against the SQL Server statement's primary output value--either the number of rows returned, or the value found in the column you specified. This script raises an event if the output value exceeds the maximum threshold or falls below the minimum threshold you set.

When constructing a SQL statement for use with this script, include the database name in the syntax. Here are some examples:

- `select categoryid from Northwind.dbo.categories`
- `use northwind select dbo.categories.categoryid from dbo.categories`

This script might encounter problems if you employ the `USE` command to qualify queries. Instead, specify `select * from mydatabase..mytable` to fully qualify queries. Do not run a command such as `use mydatabase select * from mytable`.

AppManager does not provide a syntax-checking mechanism. Syntax checking is performed by the Microsoft SQL Server on the monitored server when the job is run. If an error is detected, the Microsoft SQL Server passes an error to the Knowledge Script.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event notification	
Raise event if maximum threshold is exceeded?	Set to **Yes** to raise an event when the T-SQL statements run by this script return more rows than the threshold, or if the value in the specified column exceeds the threshold you set. The default is Yes.

Description	How to Set It
Event severity when maximum threshold exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which the maximum threshold is exceeded. The default is 15 (yellow event indicator).
Raise event if minimum threshold is not met?	Set to **Yes** to raise an event when the T-SQL statements run by this script return fewer rows than the threshold, or if the value in the specified column falls below the threshold value you set. The default is unselected.
Event severity when minimum threshold not met	Set the severity level, from 1 to 40, to indicate the importance of an event in which the minimum threshold is not met. The default is 15 (yellow event indicator).
Raise event if no rows are returned?	Set to **Yes** to raise an event if no rows are returned. The default is Yes.
Event detail options	
Include query results in event details?	Set to **Yes** to include the results of your query or command in the event detail message. By default, query results are not included.
Number of rows to display	Specify the number of rows to display in the event detail message. The default is 10 rows. **Note** You can enter 0 to indicate all rows. However, the detail message has a 32-KB limit.
Raise event for SQL Server informational messages?	Set to **Yes** to raise an event when your query generates a Microsoft SQL Server informational message. The text of the message is returned in the event detail message. This option is helpful when Microsoft SQL Server returns the query result as an informational message rather than as data. For example, when using the `dbcc checktable` command. By default, this script does not raise an event under these conditions.
Event severity for SQL Server informational messages	Set the severity level, from 1 to 40, to indicate the importance of an event in which a SQL Server information message is generated. The default is 35 (magenta event indicator).
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the script fails to run properly. The default is 5 (red event indicator).
Data Collection	
Collect data for number of rows returned?	Set to **Yes** to collect the number of rows returned by your query. If this parameter is set to **Yes** and the value returned is -1 or any negative number, an error occurred while attempting to collect data. By default, this script does not collect data.
Custom data stream legend	Specify a custom legend for the data stream returned by this Knowledge Script.
Data Detail Options	
Include query results in data details?	Set to **Yes** to include the results of your query in the data detail message. By default, query results are not included.
Number of results to display in data details	Specify the number of rows to display in the data detail message. The default is 10 rows. **Note** Enter 0 to indicate all rows. However, the detail message has a 32-KB limit.

Description	How to Set It
Monitoring	
SQL Server login	Specify the database user login that will run the SQL statements. Set this parameter to use the "sa" account, or use other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Knowledge Scripts from the AppManager for SQL Server Security Manager. **Note** In general, permission to run specific SQL commands and statements is derived from the permissions granted to the login account you are using to run this Knowledge Script. However, the `dbcc` command can only be run by: • `dbo` account (Microsoft SQL Server 2000, 2005, and 2008) • `db_backupoperator` account (Microsoft SQL Server 2000, 2005, and 2008)
SQL query or command source	Select whether you want this script or a separate file as the source of your SQL query. The possible values for this parameter are: • **Parameter**: Use the T-SQL statement you entered for the *SQL query or command statement* parameter. • **File**: Use the T-SQL statements contained in the file identified by the *Full path to SQL query or command file* parameter.
SQL query or command statement	If you are using this script as the source of your T-SQL statement, enter that statement here. You can enter only single-line statements. This parameter does not accept multi-line statements. The default is `sp_who2`. **Tip** Unless you are entering very simple statements, you might find that typing them into this field is error-prone. To avoid errors, you can copy and paste statements, or use the *Full path to SQL query or command file* parameter.
Full path to SQL query or command file	If you are using T-SQL statements contained in a file, enter the complete file path. For example, `F:\NetIQ Corporation\Sample.sql`, or \\<*computer*>\<*dir*>\`Sample.sql`. The T-SQL statements in the file must be separated by semi-colons. For more information, see "Loading SQL Server Statements From a Script File" on page 3796. You cannot use a UNC path if the NetIQ AppManager Client Resource Monitor service is running as a system account.
Threshold type	Select whether you want to perform threshold checking on one of the following: • **Number of rows returned**: Perform threshold checkin on the number of rows returned by the command or query. If the number of rows exceeds the maximum threshold or falls below the minimum threshold, an event is raised. • **Value in column number**: Perform threshold checking on the value found in a column, specified by the number of the column. Column numbers start with 0 for the leftmost column. If the value in the specified column exceeds the maximum threshold or falls below the minimum threshold, an event is raised. • **Value in column name**: Perform threshold checking on the value found in a column, specified by the name of the column. If the value in the specified column exceeds the maximum threshold or falls below the minimum threshold, an event is raised.

Description	How to Set It
Column number	If the threshold is comparing values found by column number, indicate the column number to use as the primary output value. The column you specify must contain numeric data. A value of 0 returns the first column from the SQL statements. Any other positive value returns the value for the first row of data from the specified column. If the specified column is not a numeric field, an error is raised and the Knowledge Script returns a -1 result. If you do not select by column number, you can select by column name. The default is 0. **Note** You should execute your query in SQL Query Analyzer to ensure that the proper rows and number of columns are returned. The leftmost column is column zero. Also note that if a query is doing a "`Select * ...`" and if the table schema changes, the column numbering might change.
Column name	If the threshold is comparing values found by column name, indicate the column name to use as the primary output value. The column you specify must contain numeric data. The value for the first row of data in the specified column is returned. If the specified column is not a numeric field, an error is raised and the Knowledge Script fails.
Threshold -- Maximum	Specify the maximum number of rows that can returned by the query or for the value found in the column. If the number of rows exceeds the threshold value, an event is raised. The default is 100.
Threshold -- Minimum	Specify the minimum number of rows that can be returned by the query or for the value found in the column. If the number of rows falls below the threshold value, an event is raised. The default is 0.
Save query results to a file?	Set to **Yes** to save the query results to a file. By default, query results are not saved to a file.
Full path to results file	If you are saving query results to a file, enter the complete file path and filename. For example, `F:\NetIQ Corporation\QueryResult`, or \\<*computer*>\<*dir*>\`QueryResult`. You cannot use a UNC path if the NetIQ Corporation AppManager Client Resource Monitor service is running as a system account.
Results File Content Options	
Number of rows to write to results file	Specify the number of rows to write to the result file. The default is 10.
Append to results file?	Set to **Yes** to append the results of the query to the existing contents of the results file. If disabled, the results file is overwritten each time. By default, the contents of the results file are appended each time a query or command is run.

Loading SQL Server Statements From a Script File

Because these SQL Server statements are passed through the ODBC driver, you do not need to enter the `go` statements normally required in the command line tool, `osql`. Example of a simple SQL Server script:

```
/* Script to get the number of open events. */
SELECT COUNT(*) FROM QBD.dbo.Event
WHERE ParentEventId IS NOT NULL AND Status = 0;
SELECT EventID, JobID, MachineName, KPName, Severity, Occurrence,
ModificationTime, EventMsg FROM QDB.dbo.Event
WHERE ParentEventId IS NOT NULL AND Status = 0
```

ServerDown

Use this Knowledge Script to monitor the up or down status of a Microsoft SQL Server. If the Microsoft SQL Server is down, this script raises an event and, optionally, attempts to start the Microsoft SQL Server.

This script can also identify the downtime of the Microsoft SQL Server since the server was started. This information is returned in the event detail message.

Note
The ServerDown Knowledge Script is not supported when running jobs on clusters. Use the MSCS_ResourceDown Knowledge Script to monitor a SQL Server instance on a cluster. If the MSCS (Microsoft Cluster Server) view does not exist in the AppManager console, run the Discovery_MSCS Knowledge Script on the cluster nodes.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if attempt to restart fails or succeeds?	Set to **y** to raise an event if a restart fails or succeeds. The default is y.
Collect data for server downtime?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of hours the server has been down since it was started. The default is n.
Restart SQL Server automatically if down?	Set to **y** to automatically restart Microsoft SQL Server if it is detected down. The default is y.
Event severity when attempt to restart fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager for SQL Server cannot restart it. The default is 5 (red event indicator).
Event severity when attempt to restart succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server is down and AppManager for SQL Server successfully restarted it. The default is 25 (blue event indicator).
Event severity when Restart parameter is disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server is down and the *Restart SQL Server automatically if down?* parameter has been set to "n". The default is 18 (yellow event indicator).
Raise event if the SQL Server server or agent service does not exist	Set to **y** to raise an event if the SQL Server server or agent service does not exist on the selected computer. The default is n.

ServerThroughput

Use this Knowledge Script to monitor the throughput of Microsoft SQL Server by measuring the number of T-SQL batch requests executed per second and the number of physical page reads per second.

You can set thresholds for the maximum number of batch requests or the maximum number of page reads. This script raises an event if either threshold is exceeded.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if batch requests or page reads exceed threshold?	Set to **y** to raise an event if the number of batch requests or page reads exceeds the threshold. The default is y.
Collect data for server throughput?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the throughput for Microsoft SQL Server. The default is n.
Threshold -- Maximum batch requests	Specify the maximum number of batch request transactions allowed per second before an event is raised. The default is 120.
Threshold -- Maximum page reads	Specify the maximum number of page reads allowed per second before an event is raised. The default is 100.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of batch requests or page reads exceeds the threshold. The default severity level is 5 (red event indicator).

SPIDsMonitoring

Use this Knowledge Script to monitor SQL Server Process ID (SPID) processes that run for longer than a specified time.

The SPID is assigned by Microsoft SQL Server to each new connection. SPID starts with one (1) and is globally unique.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server

Default Schedule

The default interval for this script is **Every minute**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event severity	Set the event severity level, from 1 to 30, to indicate the importance of an event in which SPID processes run for longer than the threshold you set. The default severity level is 5.
Collect data if process exceeds the threshold value	Set to **y** to collect data for charts and graphs. If enabled, data collection returns the amount of time by which SPID processes exceeded the threshold value. The default is y.
Monitoring	
SQL login	Specify the database user login account needed to access Microsoft SQL Server.
Number of processes to include in an event	Specify the maximum number of SPID processes to display in an event message. The default value is 50 SPIDs.
Units	Select the unit of time (**Hours** or **Minutes**) to be represented by the threshold value. The default is Minutes.
Threshold -- Specified time	Specify the maximum amount of time SPID processes can run before an event is raised. The default value is 500. Use the *Units* parameter to select whether the threshold represents hour or minutes.

StoredProcRecompiles

Use this Knowledge Script to monitor the number of times per second stored procedures are recompiled. This script raises an event if the stored procedure recompilation rate exceeds the threshold you set. In addition, this script generates data streams for recompilation rates.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if stored procedure recompilation rate exceeds threshold?	Set to **y** to raise an event if the recompilation rate exceeds the threshold. The default is y.
Collect data for stored procedure recompilations rate?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of times per second stored procedures were recompiled. The default is n.
Threshold -- Maximum stored procedure recompilations rate	Specify the maximum number of stored procedure recompilations per second that is allowed before an event is raised. The default is 10 recompilations per second.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the recompilation rate exceeds the threshold. The default is 5 (red event indicator).

TopCPUUsers

Use this Knowledge Script to monitor the total CPU time (in milliseconds) used by SQL Server users. This script raises an event if the value exceeds the threshold you set. In addition, this script generates data streams for CPU time usage.

You can specify the number of the highest CPU-consuming user connections to display in the event details. The event detail message includes the CPU time used, the user names of the top CPU users, the most recent SQL Server statements executed by that user, and the `spid`.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if CPU time used exceeds threshold?	Set to **y** to raise an event if CPU time usage exceeds the threshold. The default is y.
Collect data for CPU time used?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total amount of CPU time used by the top *n* CPU-consuming users. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the `sysadmin` Fixed Server Role.
Include T-SQL statements in event details?	Set to **y** to display the executing T-SQL statements in the detail message. The default is y. **Note** The executing T-SQL statements are only included in the detail message when you use the "system administrator" account.
Applications to exclude	Specify the names of the applications you do not want to monitor, separated by commas and no spaces. The default is `SQLAgent`.
Threshold -- Maximum CPU time used	Specify the maximum amount of CPU time that a user can use before an event is raised. The default is 9999999 milliseconds. **Note** This the *cumulative* CPU time for a user connection and checkpoint process.

Description	How to Set It
Number of top CPU users to include in event (0 for all)	Specify the number of top CPU-consuming users you want displayed in the detail message (event or data). Enter 0 if you want all users displayed. The default is 5.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU time usage exceeds the threshold. The default severity level is 5 (red event indicator).

TopIOUsers

Use this Knowledge Script to monitor the number of I/O read and write operations performed by Microsoft SQL Server users and their connections. This script raises an event if the number of I/O operations exceeds the threshold you set.

You can specify the number of user connections with the highest number of I/O read and write operations to display in the event detail message. The detail message includes the number of operations performed by each of the top users, their user name, the most recent SQL Server statements they executed, and their `spid`.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of I/O operations exceeds threshold?	Set to **y** to raise an event if the number of I/O operations exceeds the threshold. The default is y.
Collect data for number of I/O operations?	Set to **y** to collect data for charts and reports. If enabled, data collection, returns the number of I/O read and write operations used by SQL Server users and their connections. The event details include the user names of top I/O users, the last T-SQL statement executed, and the `spid`. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the `sysadmin` Fixed Server Role.
Include T-SQL statements in event	Set to **y** to display the executing T-SQL statements in the event detail message. The default is y. **Note** The executing T-SQL statements are only included in the detail message when you use the "system administrator" account.
Applications to exclude	Specify the names of the applications you do not want to monitor, separated by commas and no spaces. The default is `SQLAgent`.

Description	How to Set It
Threshold -- Maximum I/O operations	Specify the maximum number of I/O operations allowed by a user before an event is raised. The default is 9999999 operations. **Note** This the *cumulative* operations for a user connection.
Number of top I/O users to include in event (0 for all)	Specify the number of top I/O users to display in the event detail message. Enter 0 to display all users. The default is 5.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of I/O operations exceeds the threshold. The default severity level is 5 (red event indicator).

TopLockUsers

Use this Knowledge Script to monitor the total number of locks held by all Microsoft SQL Server users and their connections. This script raises an event if the number of user locks held exceeds the threshold you set. In addition, this script generates data streams for the number of locks held.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if locks held exceed threshold?	Set to **y** to raise an event if the number of held locks exceeds the threshold. The default is y.
Collect data for total locks held?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of locks held by SQL Server users and their connections. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the `sysadmin` Fixed Server Role.
Include T-SQL statements in event?	Set to **y** to display the executing T-SQL statements in the event detail message. The default is y. **Note** The executing T-SQL statements are only included in the detail message when you use the "system administrator" account.
Applications to exclude	Specify the names of the applications you do not want to monitor, separated by commas and no spaces. The default is `SQLAgent`.
Threshold -- Maximum user locks	Specify the maximum number of user locks allowed before an event is raised. The default is 1000 locks.

Description	How to Set It
Number of top lock users to include in event	Specify the number of top lock users to display in the detail message (event or data). The maximum allowed value is 100; minimum is 1. The default is 5 users.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of locks held exceeds the threshold. By default, the severity level is 5 (red event indicator).

TopMemoryUsers

Use this Knowledge Script to monitor the number of memory pages that can be allocated to all Microsoft SQL Server users and their connections. This script raises an event if the total number of pages allocated exceeds the threshold you set. In addition, this script generates data streams for the number of memory pages allocated.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if allocated memory exceeds threshold?	Set to **y** to raise an event if the number of allocated memory pages exceeds the threshold. The default is y.
Collect data for total memory pages allocated?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the total memory pages allocated to SQL Server users and their connections. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the `sysadmin` Fixed Server Role.
Include T-SQL statements in event?	Set to **y** to display the executing T-SQL statements in the detail message. The default is y. **Note** The executing T-SQL statements are only included in the detail message when you use the "system administrator" account.
Applications to exclude	Specify the names of the applications you do not want to monitor, separated by commas. The default is `SQLAgent`.
Threshold -- Maximum memory allocated	Specify the maximum number of memory pages that can be allocated to user connections before an event is raised. The default is 15000 pages.

Description	How to Set It
Number of top memory users to include in event (enter 0 for all)	Specify the number of top memory users to display in the detail message (event or data). Enter 0 to display all users. The default is 5.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of allocated memory pages exceeds the threshold. The default severity level is 5 (red event indicator).

TopResourceUsers

Use this Knowledge Script to monitor the total CPU time used by Microsoft SQL Server users, the number of I/O read and write operations performed by SQL Server users and their connections, the total number of locks held by all SQL Server users and their connections, and the number of memory pages that can be allocated to all SQL Server users and their connections. This script raises an event if the value exceeds the threshold you set.

This script consolidates functionality also available in four separate Knowledge Scripts: TopCPUUsers, TopIOUsers, TopLockUsers, and TopMemoryUsers. Changes to the individual scripts do not affect the functionality of this consolidated script.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Resources	
Top CPU users	Set to **Yes** to monitor the top CPU users in Microsoft SQL Server. By default, monitoring is disabled.
Top Lock users	Set to **Yes** to monitor the top lock users in Microsoft SQL Server. By default, monitoring is disabled.
Top I/O users	Set to **Yes** to monitor the top I/O users in Microsoft SQL Server. By default, monitoring is disabled.
Top Memory users	Set to **Yes** to monitor the top memory users in Microsoft SQL Server. By default, monitoring is disabled.
Event Notification	
Raise event if CPU time exceeds threshold?	Set to **Yes** to raise an event if CPU time exceeds threshold. By default, raising an event is enabled.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU time exceeds the threshold. The default severity level is 5.

Description	How to Set It
Threshold - Maximum CPU time used	Specify the maximum amount of CPU time that can be used before an event is raised. The default is 9999999 milliseconds.
Raise event if number of I/O operations exceeds threshold?	Set to **Yes** to raise an event if the number of I/O operations exceeds threshold. By default, raising an event is enabled.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of I/O operations exceeds the threshold. The default severity level is 5.
Threshold - Maximum number of I/O operations	Specify the maximum number of I/O operations that can be used before an event is raised. The default is 9999999 operations.
Raise event if number of locks held exceeds threshold?	Set to **Yes** to raise an event if the number of locks held exceeds threshold. By default, raising an event is enabled.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of locks held exceeds the threshold. The default severity level is 5.
Threshold - Maximum user locks	Specify the maximum number of user locks that can be held before an event is raised. The default is 1000 locks.
Raise event if allocated memory exceeds threshold?	Set to **Yes** to raise an event if allocated memory exceeds threshold. By default, raising an event is enabled.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which allocated memory exceeds the threshold. The default severity level is 5.
Threshold - Maximum memory allocated	Specify the maximum amount of memory that can be allocated before an event is raised. The default is 15000 pages.
Event Detail Options	
Maximum number of Top Users to include in event	Specify the maximum number of Top Users to include in the event message. The default is 10 rows. Enter 0 to display all the rows.
Data Collection	
Collect data for CPU time used?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the total amount of CPU time used by the top CPU-consuming users. By default, data collection is disabled.
Collect data for number of IO operations?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the number of I/O read and write operations used by SQL Server users and their connections. The event details include the user names of top I/O users, the last T-SQL statement executed, and the `spid`. By default, data collection is disabled.
Collect data for total locks held?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of locks held by SQL Server users and their connections. By default, data collection is disabled.
Collect data for total memory pages allocated?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns information about the total memory pages allocated to SQL Server users and their connections. By default, data collection is disabled.
Monitoring	

Description	How to Set It
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the `sysadmin` Fixed Server Role.
Applications to exclude	Specify the names of the applications you want to exclude from monitoring. Separate multiple names by commas (,) and no spaces.

UserConnections

Use this Knowledge Script to monitor the total number of Microsoft SQL Server user connections. This script raises an event if the total number of Microsoft SQL Server user connections exceeds the threshold you set.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if number of connections exceeds threshold?	Set to **y** to raise an event if the number of user connections exceeds the threshold. The default is y.
Collect data for total number of user connections?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of Microsoft SQL Server connections. The default is n.
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the `sysadmin` Fixed Server Role.
Threshold -- Maximum number of user connections	Specify the maximum number of user connections allowed before an event is raised. The default is 100 connections.
Number of connections to include in event	Specify the number of user connections to display in the event detail message. Enter 0 to display all connections. The default is 20 connections.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of user connections exceeds the threshold. The default severity level is 5 (red event indicator).

UserMaxConnection

Use this Knowledge Script to monitor the total number of Microsoft SQL Server user connections and the opened connection usage of Microsoft SQL Server.

This script consolidates functionality also available in two separate Knowledge Scripts: NearMaxConnect and UserConnections. Changes to the individual scripts do not affect the functionality of this consolidated script.

Note
This script does not raise events or generate data points when it runs on a computer that is part of a cluster but is not the node owner. Run the ClusterOwner Knowledge Script to determine which computer owns the node.

Version Compatibility

Microsoft SQL Server 2000, 2005, and 2008

Resource Object

Microsoft SQL Server folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if number of connections exceeds threshold?	Set to **Yes** to raise events if the number of user connections exceeds threshold. The default is Yes.
Event severity when number of user connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of user connections exceeds the threshold. The default severity level is 5.
Threshold -- Maximum number of user connections	Specify the maximum number of user connections allowed before an event is raised. The default is 100 connections.
Raise event if used connections exceeds threshold?	Set to **Yes** to raise events if the number of used connections exceeds threshold. The default is Yes.
Event severity when number of used connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of used connections exceeds the threshold. The default severity level is 5.
Threshold -- Maximum percentage of connections used	Specify the maximum percentage of user connections allowed before an event is raised. The default is 0%.
Data Collection	

Description	How to Set It
Collect data for total number of user connections?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of Microsoft SQL Server connections. The default is Yes.
Collect data for number of connections used?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns the total number of used Microsoft SQL Server connections. The default is Yes.
Monitoring	
SQL Server login	Specify the database user login account needed to access Microsoft SQL Server. Use the "`sa`" account or other user login accounts that have been set up in the Microsoft SQL Server on the managed client and have been given permission to run SQL Server Knowledge Scripts through AppManager Security Manager. **Note** The account must be in the `sysadmin` Fixed Server Role.

Chapter 67
SQL-RT Knowledge Scripts

AppManager ResponseTime for Microsoft SQL Server provides Knowledge Scripts for monitoring SQL Server response time.

The ADO Knowledge Scripts use Microsoft ActiveX Data Objects (ADO) that are built on the top of Microsoft OLE Database (OLEDB). If you are using ADO or OLEDB on production, you may find it inappropriate to use ODBC to evaluate client/server database performance.

The SQL-RT category of Knowledge Scripts support both ODBC and ADO. You can set ADO parameters to match those in the applications you are testing. You should be able to configure an ADO Knowledge Script in the same way you configure an `ADODB::Connection` on an in-house application.

ADO and ODBC Knowledge Scripts support SQL statements. Be aware that some risk exists in doing continuous `INSERT` and `DELETE` statements on a short schedule.

These Knowledge Scripts support both System and User DSN. Use the appropriate Knowledge Script for the application you are testing.

From within the SQL-RT view of the Operator Console, you can select a Knowledge Script on the **SQL-RT** tab of the Knowledge Script pane. The following are the Knowledge Scripts in the SQL-RT category:

Knowledge Script	What It Does
ADODSNQuery	Queries a Microsoft SQL Server using ADO and a system DSN.
ADOQuery	Queries a Microsoft SQL Server using ADO.
AdvancedADOQuery	Queries a Microsoft SQL Server using ADO and advanced connection parameters.
ODBCDSNQuery	Queries a Microsoft SQL Server using ODBC DSN.
ODBCQuery	Queries a Microsoft SQL Server using ODBC.
Report_SQL-RT	Summarizes availability and response time for SQL-RT Knowledge Scripts.
Report_SQL-RT_DSN	Summarizes availability and response time for the SQL-RT Knowledge Scripts that use DSN.

ADODSNQuery

Use this Knowledge Script to query a Microsoft SQL Server using ActiveX Data Objects (ADO) and a system Data Source Name (DSN).

This script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to three response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed.
- **Availability.** This data stream returns one of two values, depending on the data stream format you selected:
  - 1 or 100 = transaction was successful
  - 0 = transaction was not successful

  The Availability data point is an indication of whether the transaction succeeded or failed.

This script raises an event whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The SQL-RT engine cannot be initialized. An initialization error is raised, but neither an Availability nor a Response Time data stream is generated.
- The job transaction does not complete successfully. A transaction error is raised. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console.

Resource Object

The SQL response time ADO client

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Windows Authentication

The ADOQuery and AdvancedADOQuery Knowledge Scripts support both SQL Server authentication and Windows authentication; however, the ADODSNQuery Knowledge Script is limited using the security settings in the DSN configuration because ADO cannot overwrite this kind of DSN setting.

Therefore, the job may not use the type of authentication you expected it to use. For example, say you set an invalid SQL username and/or password for the ADODSNQuery parameters, but the job still runs successfully. This can happen when the DSN is set to use Windows authentication, also called "integrated security.". In such a case, if the *Run As Username* parameter has appropriate privileges on the SQL Server database, the OLEDB driver ignores the specific logon user and password supplied in the Knowledge Script parameters. The logon works because the Windows authentication configured in the DSN takes precedence over the SQL Server authentication specified in the Knowledge Script.

Setting Parameter Values

When running this script, use the security model that was set when you defined the DSN.

- When using a DSN configured to use SQL authentication, use the *SQL Logon Username* and *Password* parameters. Or specify a valid Windows account for the *Run As* parameters.
- When using a DSN defined with Windows NT authentication, leave the *SQL Logon Username* and *Password* parameters blank, and specify the valid Windows account for the *Run As* parameters.

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select **Yes** to collect data for graphs and reports. If enabled, data collection returns: • 1 or 100 -- Transaction completed successfully • 0 -- Transaction did not complete successfully • Time taken to execute the query (in seconds) The default is Yes.
Data stream format	Select a format for the Availability data stream. You can select a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if transaction fails?	Select **Yes** to raise an event when the server cannot be contacted. The default is Yes.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server cannot be contacted. The default is 5.
Response Time	
Collect data for response time?	Select **Yes** to collect response-time data for graphs and reports. The default is Yes. If you enable data collection, you also have the option to see a breakdown in the response times for the component parts of the query, such as the time taken to connect to the SQL Server.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The default is 15 seconds.
Raise event if threshold is exceeded?	Select **Yes** to raise an event when the threshold is exceeded. The event message contains a breakdown of the total response time. The default is Yes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which response time exceeds the threshold. The default is 15.
Response Time Breakdown	
Collect data for connecting to SQL Server?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to establish a connection to the SQL Server. The default is unselected.

Description	How to Set It
Collect data for executing SQL statement?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to execute the SQL statement. The default is unselected.
Collect data for fetching data?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to perform a `fetch` of the query data. The default is unselected.
Target computer	Provide the computer name and instance of the SQL Server. This is an optional field, and is used to enable retrieval of data streams by AppManager Analysis Center v2.0 and later. If specified, it will also be used in place of the DSN in the data stream legend. If you set the *Event on* parameter, the *Target computer* parameter lets you select the server where the event will appear in your console. Enter the name of the server, or click **Browse [...]** to select from a list of available servers. The server you select must already be in the TreeView.
Data source (DSN)	Provide the Data Source DSN used for the connection.
Attributes	Specify the `ADODB::Connection` attributes as follows: • `NONE` (the default). No attributes. • `ABORTRETAINING`: Performs retaining aborts; i.e., calls `RollbackTrans` and automatically starts a new transaction. Not supported by all providers. • `COMMITRETAINING`: Performs retaining commits; i.e., calls `CommitTrans` and automatically starts a new transaction. Not supported by all providers. • `ABORTCOMITRETAINING`: A combination of `ABORTRETAINING` and `COMMITRETAINING`.
Cursor location	Specify the location of the cursor service: • `CLIENT`: Uses client-side cursors supplied by a local cursor library. (Local services may allow many features not allowed by driver-supplied cursors; using this setting may provide some advantage in enabling features.) • `SERVER`: Uses data provider- or driver-supplied cursors. (These cursors may be flexible and allow for additional sensitivity to changes made to the data source by others.) This is the default.
SQL statement	Provide a SQL statement (1024-character maximum) that is compatible with the provider. Calling stored procedures is also supported. The format is `execute stored_procedure`.
Number of rows per fetch	Specify any positive integer or -1. Use an appropriate value according to the size of the result and of a single row. The default value is 1. If the SQL statement is a select, the engine uses the `GetRows()` method to retrieve the data, so you can fetch thousands or records at once. This could mean a huge performance improvement in production. A value of -1 attempts to retrieve all rows on a single fetch. Although this may show interesting results on a small database, it can easily become catastrophic if the result is large and the client machine has limited memory. You should change this value only if the `GetRows ()` method is used in production with a value different than 1.

Description	How to Set It
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** (the client computer in the response-time tests). This is the default. • **Server** (the SQL server being tested--see the **Target computer** parameter, above) • **Both.** The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
SQL Logon	
Username	Set this value appropriately based upon your DSN settings.
Password	Set this value appropriately based upon your DSN settings.
Run As	
Username	Provide the username associated with a specific user who has the required permissions to run this application. **Required**. `Interactive User` is a possible value. Leave the Password and Domain parameters blank if you specify "Interactive User". `Interactive User` requires a user to be physically logged into the computer for the test to run. You might want to do this in environments where a firewall is preventing access to an Active Directory domain controller, or where the test computer is part of a workgroup and not part of a domain. With this feature, the user is not validated, so the test can proceed despite the lack of access to the domain.
Password	Specify the password associated with this user that is required to log on to the network and run the application.
Domain	Specify the domain associated with this user that is the domain name you are logging onto. **Required**.
Administrators group on managed client	Provide the name of the Administrators Group on the managed client. Typically, this name is “`Administrators`”, except on some foreign language operating systems. The default is “`Administrators`”.
Timeouts	
Command timeout	Specify the number of seconds to wait while establishing a connection before terminating the event and raising an event. The default is 30 seconds.
Connection timeout	Specify the number of seconds to wait while executing a command before terminating the attempt and raising an event. The default is 15 seconds.

ADOQuery

Use this Knowledge Script to query a Microsoft SQL Server using ADO.

This script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to three response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. See "Setting Parameter Values" on page 3817 below for more information.
- **Availability**–Returns one of two values:
  - 1 or 100 = transaction was successful
  - 0 = transaction was not successful.

  The Availability data point is an indication of whether the transaction succeeded or failed.

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The SQL-RT engine cannot be initialized. An initialization error is raised, but neither an Availability nor a Response Time data stream is generated.
- The job transaction doesn't complete successfully. A transaction error is raised. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console.

Resource Object

The SQL-RT ADO client

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Windows Authentication

The ADOQuery and AdvancedADOQuery Knowledge Scripts support both SQL Server authentication and Windows authentication; however, the ADODSNQuery Knowledge Script is limited to the DSN configuration because ADO cannot override this kind of DSN setting.

Therefore, the job may not use the type of authentication you expected it to use. For example, say you set an invalid SQL username and/or password for ADODSNQuery Knowledge Script parameters. The job may still run successfully if the DSN is set to use Windows authentication. In such a case, if the *Run As Username* parameter has appropriate privileges on the SQL Server database, the OLEDB driver ignores the specific logon username and password. The logon always works because the Windows authentication configured in the DSN takes precedence over the SQL Server authentication set in the Knowledge Script.

Setting Parameter Values

Set the Integrated security option according to the security model you want to use:

- **For SQL authentication**: Clear the **Yes** check box to disable integrated security, then specify the SQL Logon Username and Password parameters. Also, specify the *Run As* parameters to supply a valid account under which to run the Knowledge Script.
- **For Windows authentication**: Select the **Yes** check box for integrated security, and leave the *SQL Username* and *Password* parameters blank. Specify the valid account under which to run the Knowledge Script and perform the Windows authentication for the *Run As* parameters.

Set the following parameters as needed.

Description	How to Set It
Availability	
Collect data for availability?	Select **Yes** to collect data for graphs and reports. If enabled, data collection returns: • 1 or 100 -- Transaction completed successfully • 0 -- Transaction did not complete successfully • Time taken to execute the query (in seconds) The default is Yes.
Data stream format	Select a format for the Availability data stream. You can select a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if transaction fails?	Select **Yes** to raise an event when the server cannot be contacted. The default is yes.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server cannot be contacted. The default is 5.
Response Time	
Collect data for response time?	Select **Yes** to collect response-time data for graphs and reports. The default is Yes. If you enable data collection, you also have the option to see a breakdown in the response times for the component parts of the query, such as the time taken to connect to the SQL Server.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The default is 15 seconds.
Raise event if threshold is exceeded?	Select **Yes** to raise an event when the threshold is exceeded. The event message contains a breakdown of the total response time. The default is Yes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which response time exceeds the threshold. The default is 15.
Response Time Breakdown	
Collect data for connecting to SQL Server?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to establish a connection to the SQL Server. The default is unselected.
Collect data for executing SQL statement?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to execute the SQL statement. The default is unselected.
Collect data for fetching data?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to perform a `fetch` of the query data. The default is unselected.

Description	How to Set It
Server and instance name	Provide the names of the server and instance where the transaction will be run. Use the following syntax: `Server/Instance`. If you set the *Event on* parameter, this parameter lets you select the server where the event will appear in your console. The instance name is stripped out. Provide the name of the server and instance, or click **Browse [...]** to select from a list of available servers. The server you select must already be in the TreeView.
Database name	Specify the database name on the SQL Server. This is the “Initial Catalog” part of the Connection Properties collection. If the provider does not support this property, use the default database.
Cursor location	Specify the location of the cursor service: • `CLIENT`: Uses client-side cursors supplied by a local cursor library. (Local services may allow many features not allowed by driver-supplied cursors; using this setting may provide some advantage in enabling features.) • `SERVER`: Uses data provider- or driver-supplied cursors. (These cursors may be flexible and allow for additional sensitivity to changes made to the data source by others.) This is the default.
SQL statement	Provide a SQL statement (128-character maximum) that is compatible with the provider. The format is `execute stored_procedure`.
Number of rows per fetch	Specify any positive integer or -1. Use an appropriate value according to the size of the result and of a single row. The default value is 1. If the SQL statement is a select, the engine uses the `GetRows()` method to retrieve the data, so you can fetch thousands or records at once. This could mean a huge performance improvement in production. A value of -1 attempts to retrieve all rows on a single fetch. Although this may show interesting results on a small database, it can easily become catastrophic if the result is large and the client computer has limited memory. Change this value only if the `GetRows()` method is used in production with a value different than 1.
Integrated security?	Select **Yes** to specify whether the authentication should be done on the Windows integrated security model. The default is unselected.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** (the client computer in the response-time tests). This is the default. • **Server** (the SQL server being tested--see the *Server and instance name* parameter) • **Both.** The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
SQL Logon	
Username	Set this value when you do *not* use integrated security. This is the User ID part of the Connection Properties collection.
Password	Set this value when you do *not* use integrated security. This is the Password part of the Connection Properties collection. Hard encryption is always used.
Run As	

Description	How to Set It
Username	Provide the username associated with a specific user who has the required permissions to run this application. **Required**. `Interactive User` is a possible value. Leave the Password and Domain parameters blank if you specify "Interactive User". `Interactive User` requires a user to be physically logged into the computer for the test to run. You might want to do this in environments where a firewall is preventing access to an Active Directory domain controller, or where the test computer is part of a workgroup and not part of a domain. With this feature, the user is not validated, so the test can proceed despite the lack of access to the domain.
Password	Provide the password associated with this user that is required to log on to the network and run the application.
Domain	Provide the domain associated with this user that is the domain name you are logging onto. **Required**.
Administrators group on managed client	Provide the name of the Administrators Group on the managed client. Typically, this name is “`Administrators`”, except on some foreign-language operating systems. The default is “`Administrators`”.
Timeouts	
Command timeout	Specify the number of seconds to wait while establishing a connection before terminating the event and generating an error. The default is 30 seconds.
Connection timeout	Specify the number of seconds to wait while executing a command before terminating the attempt and generating an error. The default is 15 seconds.

AdvancedADOQuery

Use this Knowledge Script to check the ability to query a Microsoft SQL Server using ADO and advanced connection parameters.

This script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to three response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. See "Setting Parameter Values" on page 3817 below for more information.
- **Availability**–Returns one of two values:
  - 1 or 100 = transaction was successful
  - 0 = transaction was not successful.

  The Availability data point is an indication of whether the transaction succeeded or failed.

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The SQL-RT engine cannot be initialized. An initialization error is raised, but neither an Availability nor a Response Time data stream is generated.
- The job transaction does not complete successfully. A transaction error is raised. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console.

Resource Object

The SQL response time ADO client

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Be sure to set the *Integrated security?* parameter according to the security model you want to use:

- **For SQL authentication:** Clear the **Yes** check box to disable integrated security, then specify the *SQL Logon Username* and *Password*. Also specify the *Run As* account information to supply a valid account under which to run the Knowledge Script.
- **For Windows authentication:** Select the **Yes** check box for integrated security, and leave the *SQL Logon Username* and *Password* parameters blank. Specify a valid user account under which to run the Knowledge Script for the *Run As* Knowledge Script parameters.

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select **Yes** to collect data for graphs and reports. If enabled, data collection returns: • 1 or 100 -- Transaction completed successfully • 0 -- Transaction did not complete successfully • Time taken to execute the query (in seconds) The default is Yes.
Data stream format	Select the data stream format for the Availability data stream. You can use a 0 (“not available”) or 100 (“available”) format. The default value is 0-100.
Raise event if transaction fails?	Select **Yes** to raise an event when the server cannot be contacted. The default is Yes.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server cannot be contacted. The default is 5.
Response Time	
Collect data for response time?	Select **Yes** to collect response-time data for graphs and reports. By default, data is collected. If you enable data collection, you also have the option to see a breakdown in the response times for the component parts of the query, such as the time taken to connect to the SQL Server.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The default is 15 seconds.
Raise event if threshold is exceeded?	Select **Yes** to raise an event when the threshold is exceeded. The event message contains a breakdown of the total response time. The default is Yes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the response time threshold is exceeded. The default is 15.
Response Time Breakdown	
Collect data for connecting to SQL Server?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to establish a connection to the SQL Server. The default is unselected.
Collect data for executing SQL statement?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to execute the SQL statement. The default is unselected.
Collect data for fetching data?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to perform a `fetch` of the query data. The default is unselected.
Server and instance name	Provide the names of the server and instance where the transaction will be run. Use the following syntax: `Server/Instance`. If you set the *Event on* parameter, this parameter lets you select the server where the event will appear in your console. The instance name is stripped out. Provide the name of the server and instance, or click **Browse [...]** to select from a list of available servers. The server you select must already be in the TreeView.
Database name	Provide the database name on the SQL Server. This is the “Initial Catalog” part of the Connection Properties collection. If the provider does not support this property, use the default database.

Description	How to Set It
Attributes	Specify the `ADODB::Connection` attributes as follows: • `NONE` (the default). No attributes. • `ABORTRETAINING`: Performs retaining aborts; i.e., calls `RollbackTrans` and automatically starts a new transaction. Not supported by all providers. • `COMMITRETAINING`: Performs retaining commits; i.e., calls `CommitTrans` and automatically starts a new transaction. Not supported by all providers. • `ABORTCOMITRETAINING`: A combination of `ABORTRETAINING` and `COMMITRETAINING`.
Cursor location	Specify the location of the cursor service: • `CLIENT`: Uses client-side cursors supplied by a local cursor library. (Local services may allow many features not allowed by driver-supplied cursors; using this setting may provide some advantage in enabling features.) • `SERVER`: Uses data provider- or driver-supplied cursors. (These cursors may be flexible and allow for additional sensitivity to changes made to the data source by others.) This is the default.
Isolation level	Specify the level of transaction isolation for a Connection object as follows: • `UNSPECIFIED`: The provider is using a different isolation level than specified, but that level cannot be determined. • `CHAOS`: You cannot overwrite pending changes from more highly isolated transactions. • `BROWSE`: You can view uncommitted changes in other transactions from one transaction. • `READUNCOMMITTED`: Same as `BROWSE`. • `CURSORSTABILITY`: You can view changes in other transactions from one transaction only after they have been committed. • `READCOMMITTED`: Same as `BROWSE`. This is the default. • `REPEATABLEREAD`: You cannot see changes made in other transactions from one transaction; however, querying again can retrieve new `Recordset` objects. • `ISOLATED`: Transactions are conducted in isolation from other transactions. • `SERIALIZABLE`: Same as `ISOLATED`.
Mode	Set the available permissions for modifying data in a connection, as follows: • `UNKNOWN`: Permissions have either not yet been set or cannot be determined. This is the default. • `READ`: Read-only permissions. • `WRITE`: Write-only permissions. • `READWRITE`: Read/write permissions. • `RECURSIVE`: Not supported at this time. • `SHAREDENYNONE`: Allows others to open a connection with any permission. Neither read nor write access can be denied to others. • `SHAREDENYREAD`: Prevents others from opening a connection with read permissions. • `SHAREDENYWRITE`: Prevents others from opening a connection with write permissions. • `SHAREEXCLUSIVE`: Prevents others from opening a connection.
SQL Statement	Provide a SQL statement (128-character maximum) that is compatible with the provider. The format is `execute stored_procedure`.

Description	How to Set It
Number of rows per fetch	Specify any positive integer or -1. Use an appropriate value according to the size of the result and of a single row. The default value is 1. If the SQL statement is a select, the engine uses the `GetRows()` method to retrieve the data, so you can fetch thousands or records at once. This could mean a huge performance improvement in production. A value of -1 attempts to retrieve all rows on a single fetch. Although this may show interesting results on a small database, it can easily become catastrophic if the result is large and the client machine has limited memory. You should change this value only if the `GetRows()` method is used in production with a value different than 1.
Integrated security?	Select **Yes** to specify whether the authentication should be done on the Windows integrated security model. The default is unselected.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** (the client computer in the response-time tests). This is the default. • **Server** (the SQL server being tested--see the *Server and instance name* parameter) • **Both.** The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
SQL Logon	
Username	Set this value when you do *not* use integrated security. This is the User ID part of the Connection Properties collection.
Password	Set this value when you do *not* use integrated security. This is the Password part of the Connection Properties collection. Hard encryption is always used.
Run As	
Username	Provide the username associated with a specific user who has the required permissions to run this application. **Required**. `Interactive User` is a possible value. Leave the Password and Domain parameters blank if you specify "Interactive User". `Interactive User` requires a user to be physically logged into the computer for the test to run. You might want to do this in environments where a firewall is preventing access to an Active Directory domain controller, or where the test computer is part of a workgroup and not part of a domain. With this feature, the user is not validated, so the test can proceed despite the lack of access to the domain.
Password	Provide the password associated with this user that is required to log on to the network and run the application.
Domain	Provide the domain associated with this user that is the domain name you are logging onto. **Required**.
Administrators group on managed client	Enter the name of the Administrators Group on the managed client. Typically, this name is “`Administrators`”, except on some foreign-language operating systems. The default is “`Administrators`”.
Timeouts	
Command timeout	Specify the number of seconds to wait while establishing a connection before terminating the event and generating an error. The default is 30 seconds.

Description	How to Set It
Connection timeout	Specify the number of seconds to wait while executing a command before terminating the attempt and generating an error. The default is 15 seconds.

ODBCDSNQuery

Use this Knowledge Script to query a Microsoft SQL Server using Open Database Connectivity (ODBC) and a Data Source Name (DSN).

This script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to three response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. See "Setting Parameter Values" on page 3817 below for more information.
- **Availability**–Returns one of two values:
  - 1 or 100 = transaction was successful
  - 0 = transaction was not successful.

  The Availability data point is an indication of whether the transaction succeeded or failed.

This script raises an event whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The SQL-RT engine can't be initialized. An initialization error is raised, but neither an Availability nor a Response Time data stream is generated.
- The job transaction doesn't complete successfully. A transaction error is raised. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console.

Resource Object

The SQL response time ODBC client

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

About Windows Authentication

ODBC Knowledge Scripts do not support Windows authentication (integrated security), but DSN does. Therefore, the job may not use the type of authentication you wanted it to use. For example, if you set an invalid SQL username and/or password in the ODBCDSNQuery Knowledge Script, the job may run successfully if the DSN is set to use Windows authentication.

In such a case, if the value supplied for the *Run As Username* parameter has appropriate privileges on the SQL Server database, the ODBC driver ignores the specific logon username and password you supplied. The logon then succeeds in this case because the Windows authentication in the DSN takes precedence over the authentication method set in the Knowledge Script.

Setting Parameter Values

Depending on what security model was set when you defined the DSN, you should only use that security method when running this Knowledge Script.

- When using a DSN defined with SQL authentication, use the *SQL Logon Username* and *Password* fields only.
- When using a DSN configured to use Windows authentication, leave the *SQL Logon Username* and *Password* fields blank, and specify the valid Windows account for the *Run As* Knowledge Script parameters.

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select **Yes** to collect data for graphs and reports. If enabled, data collection returns: • 1 or 100 -- Transaction completed successfully • 0 -- Transaction did not complete successfully • Time taken to execute the query (in seconds) The default is yes.
Data stream format	Select the data stream format for the Availability data stream. You can use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if transaction fails?	Select **Yes** to raise an event when the server cannot be contacted. The default is Yes.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server cannot be contacted. The default is 5.
Response Time	
Collect data for response time?	Select **Yes** to collect response time data for graphs and reports. The default is Yes. If you enable data collection, you also have the option to see a breakdown in the response times for the component parts of the query, such as the time taken to connect to the SQL Server.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The default is 15 seconds.
Raise event if threshold is exceeded?	Select **Yes** to raise an event when the threshold is exceeded. The event message contains a breakdown of the total response time. The default is Yes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which response time exceeds the threshold. The default is 15.
Response Time Breakdown	
Collect data for connecting to SQL Server?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to establish a connection to the SQL Server. The default is unselected.
Collect data for executing SQL statement?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to execute the SQL statement. The default is unselected.
Collect data for fetching data?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to perform a `fetch` of the query data. The default is unselected.

Description	How to Set It
Target computer	Specify the computer name and instance of the SQL Server. This is an optional field, and is used to enable retrieval of data streams by AppManager Analysis Center v2.0 and later. If specified, it is also used in place of the DSN in the data stream legend. If you set the *Event on* parameter, the *Target computer* parameter lets you select the server where the event will appear in your console. Specify the name of the server and instance, or click **Browse [...]** to select from a list of available servers. The server you select must already be in the TreeView.
Data source (DSN)	Provide the system DSN on which the Knowledge Script will be run. **Required**.
SQL Statement	Provide a SQL statement (128-character maximum) that is compatible with the provider. The format is `execute stored_procedure`.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** (the client computer in the response-time tests). This is the default. • **Server** (the SQL server being tested--see the *Target computer* parameter) • **Both.** The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
SQL Logon	
Username	Set this value appropriately based upon your DSN settings.
Password	Set this value appropriately based upon your DSN settings.
Run As	
Username	Provide the username associated with a specific user who has the required permissions to run this application. **Required**. `Interactive User` is a possible value. Leave the Password and Domain parameters blank if you specify "Interactive User". `Interactive User` requires a user to be physically logged into the computer for the test to run. You might want to do this in environments where a firewall is preventing access to an Active Directory domain controller, or where the test computer is part of a workgroup and not part of a domain. With this feature, the user is not validated, so the test can proceed despite the lack of access to the domain.
Password	Provide the password associated with this user that is required to log on to the network and run the application.
Domain	Provide the domain associated with this user that is the domain name you are logging onto. Required.
Administrators group on managed client	Provide the name of the Administrators Group on the managed client. Typically, this name is “`Administrators`”, except on some foreign language operating systems. The default is “`Administrators`”.
Connection timeout	Specify the number of seconds to wait while executing a command before terminating the attempt and generating an error. The default is 15 seconds.

ODBCQuery

Use this Knowledge Script to query a Microsoft SQL Server using Open Database Connectivity (ODBC) and measure the response time.

This script does not support Windows authentication. Use the ODBCDSNQuery Knowledge Script if you need to use Windows authentication. That script lets you supply a DSN to use. You can then configure the Data Source Name (DSN) file to use Windows authentication.

This script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to three response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. See "Setting Parameter Values" on page 3817 below for more information.
- **Availability**–Returns one of two values:
  - 1 or 100 = transaction was successful
  - 0 = transaction was not successful.

  The Availability data point is an indication of whether the transaction succeeded or failed.

This script raises an event whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The SQL-RT engine cannot be initialized. An initialization error is raised, but neither an Availability nor a Response Time data stream is generated.
- The job transaction does not complete successfully. A transaction error is raised. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console.

Resource Object

The SQL response time ODBC client.

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	

Description	How to Set It
Collect data for availability?	Select **Yes** to collect data for graphs and reports. If enabled, data collection returns: • 1 or 100 -- Transaction completed successfully • 0 -- Transaction did not complete successfully • Time taken to execute the query (in seconds) The default is Yes.
Data stream format	Select a format for the Availability data stream. You can use a 0 (“not available”) or 100 (“available”) format. The default value is 0-100.
Raise event if transaction fails?	Select **Yes** to raise an event when the server cannot be contacted. The default is Yes.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the server cannot be contacted. The default is 5.
Response Time	
Collect data for response time?	Select **Yes** to collect response time data for graphs and reports. The default is Yes. If you enable data collection, you also have the option to see a breakdown in the response times for the component parts of the query, such as the time taken to connect to the SQL Server.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The default is 15 seconds.
Raise event if threshold is exceeded?	Select **Yes** to raise an event when the threshold is exceeded. The event message contains a breakdown of the total response time. The default is Yes.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which response time exceeds the threshold. The default is 15.
Response Time Breakdown	
Collect data for connecting to SQL Server?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to establish a connection to the SQL Server. The default is unselected.
Collect data for executing SQL statement?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to execute the SQL statement. The default is unselected.
Collect data for fetching data?	Select **Yes** to collect response-time data showing how much of the overall response time could be attributed to the time taken to perform a `fetch` of the query data. The default is unselected.
Server and instance name	Provide the names of the server and instance where the transaction will be run. Use the following syntax: `Server/Instance`. If you set the *Event on* parameter, this parameter lets you select the server where the event will appear in your console. The instance name is stripped out. Provide the name of the server and instance, or click **Browse [...]** to select from a list of available servers. The server you select must already be in the TreeView.
Database name	Provide the database name on the SQL Server. This is the “Initial Catalog” part of the Connection Properties collection. If the provider does not support this property, use the default database.
SQL statement	Set this value appropriately based on your DSN settings. The format is `execute stored_procedure`.

Description	How to Set It
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** (the client computer in the response-time tests). This is the default. • **Server** (the SQL server being tested--see the **Server and instance name** parameter, above) • **Both.** The event will be shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
SQL Logon	
Username	Set this value appropriately based on your DSN settings.
Password	Set this value appropriately based on your DSN settings.
Run As	
Username	Provide the username associated with a specific user who has the required permissions to run this application. **Required**. `Interactive User` is a possible value. Leave the Password and Domain parameters blank if you specify "Interactive User". `Interactive User` requires a user to be physically logged into the computer for the test to run. You might want to do this in environments where a firewall is preventing access to an Active Directory domain controller, or where the test computer is part of a workgroup and not part of a domain. With this feature, the user is not validated, so the test can proceed despite the lack of access to the domain.
Password	Provide the password associated with this user that is required to log on to the network and run the application.
Domain	Provide the domain associated with this user that is the domain name you are logging onto. **Required**.
Administrators group on managed client	Provide the name of the Administrators Group on the managed client. Typically, this name is “`Administrators`”, except on some foreign language operating systems. The default is “`Administrators`”.
Connection timeout	Specify the number of seconds to wait while executing a command before terminating the attempt and generating an error. The default is 15 seconds.

Report_SQL-RT

Use this Report Knowledge Script to generate a report detailing availability and response time for the following SQL-RT Knowledge Scripts:

- ADOQuery
- AdvancedADOQuery
- ODBCQuery

Resource Object

AppManager repository

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
KS for report	Click **Browse [...]** to select the Knowledge Scripts you want to include in the report.
SQL-RT client(s)	Click **Browse [...]** to select the SQL-RT client computers to include in the report. Your selections are limited to computers or server groups that are visible in the selected views. Select one of the filter options: • **View:** Includes all computers in the views you selected. • **Computer:** Select from individual computers in the views you selected. • **Server Group:** Select from server groups in the views you selected. **Note** Selecting a server group includes all computers in that group.
SQL Server or "All"	Specify the name of the SQL Server or type "All" to designate all computers as SQL Servers. The default is "All".
Select time range	Click **Browse [...]** to set specific start and end report information dates, good for historical or ad hoc reports, or a sliding range that sets the time range of data to include in the report. The sliding range option is the default and is useful for reports running on a regular schedule.
Select peak weekday(s)	Click **Browse [...]** to select a contiguous day range a selection of non-contiguous days.
Aggregation by	Select the time unit by which to aggregate data. The default is Hour. This works in conjunction with the *Aggregation interval* parameter, which determines the number of units for one interval of data aggregation.
Aggregation interval	Select the interval units in which to aggregate data. The default is 1. For example, if you aggregate by the Hour and select 1 here, data is aggregated once every hour.
Report Settings	
Include parameter card?	Select **Yes** to display a table of parameters used in the report. The default is Yes.

Description	How to Set It
Include Availability Detail table?	Select **Yes** to display the Availability Detail table as part of the report. The default is Yes.
Include Availability chart?	Select **Yes** to display the Availability chart as part of the report. The default is Yes.
Availability data stream format	Specify the data stream format. Options are 0-100 or 0-1. • 1 or 100 -- Available • 0 -- Not available The default format is 0-100.
Threshold on Availability chart	Specify an integer for the percentage threshold. The default is 0 (no threshold is displayed).
Include Response Time Detail table?	Select **Yes** to display the Response Time detail table as part of the report. The default is Yes.
Include Response Time chart?	Select **Yes** to display the Response Time chart as part of the report. The default is Yes.
Units for Response Time report	Select the response time unit, msec or sec. The default is msec.
Threshold on Response Time chart (selected units)	Specify the response time threshold to display on the chart in the report. The default is 0, which suppresses the threshold indicator in the chart.
Select chart style	Click **Browse [...]** to set the appearance of the chart. The same parameters are used in both the Availability and Response Time charts, if both are produced. The default is Ribbon.
Select output folder	Select **Browse [...]** to specify the report filename and the report folder. You can specify a specific folder or have the system generate the folder each time the report runs.
Add job ID to output folder name?	Select **Yes** to add a job ID to the output folder name. Use a job ID to correlate a specific instance of a Report Script with the corresponding report. The default is unselected.
Index-Report Title	Select **Browse [...]** to configure report title settings and custom fields.
Add timestamp to title?	Select **Yes** to add a timestamp to the report title, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is unselected.
Event Notification	
Generate event on success?	Select **Yes** to raise an event when a report is generated. The default is Yes.
Severity level for report success	Set the event severity level to indicate the importance of an event in which the report is generated successfully. The default is 35.
Severity level for report with no data	Set the event severity level to indicate the importance of an event in which the report has no data. The default is 25.
Severity level for report failure	Set the event severity level to indicate the importance of an event in which the report cannot be generated. The default is 5.

Report_SQL-RT_DSN

Use this Report Knowledge Script to generate a report detailing availability and response time for the following SQL-RT DSN Knowledge Scripts:

- ADODSNQuery
- ODBCDSNQuery

Resource Object

AppManager repository

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
KS for report	Click **Browse [...]** to select the Knowledge Scripts you want to include in the report.
SQL-RT client(s)	Click **Browse [...]** to select the SQL-RT client computers to include in the report. Your selections are limited to computers or server groups that are visible in the selected views. Select one of the filter options: • **View:** Includes all computers in the views you selected. • **Computer:** Select from individual computers in the views you selected. • **Server Group:** Select from server groups in the views you selected. **Note** Selecting a server group includes all computers in that group.
SQL DSN or "All"	Specify the name of the SQL Server or type "All" to designate all computers as SQL Servers. The default is "All".
Select time range	Click **Browse [...]** to set specific start and end report information dates, good for historical or ad hoc reports, or a sliding range that sets the time range of data to include in the report. The sliding range option is the default and is useful for reports running on a regular schedule.
Select peak weekday(s))	Click **Browse [...]** to select a contiguous day range a selection of non-contiguous days.
Aggregation by	Select the time unit by which to aggregate data. The default is Hour. This works in conjunction with the next field (Aggregation interval), which determines the number of units for one interval of data aggregation.
Aggregation interval	Select the interval units in which to aggregate data. The default is 1. For example, if you aggregate by the Hour and select 1 here, data is aggregated once every hour.
Report Settings	
Include parameter card?	Select **Yes** to display a table of parameters used in the report. The default is Yes.
Include Availability detail table?	Select **Yes** to display the Availability Detail table as part of the report. The default is Yes.

Description	How to Set It
Include Availability chart?	Select **Yes** to display the Availability chart as part of the report. The default is Yes.
Availability data stream format	Specify the data stream format. Options are 0-100 or 0-1. • 1 or 100 -- Available • 0 -- Not available The default format is 0-100.
Threshold on Availability chart	Specify an integer for the percentage threshold. The default is 0 (no threshold is displayed).
Include Response Time Detail table?	Select **Yes** to display the Response Time Detail table as part of the report. The default is Yes.
Include Response Time chart?	Select **Yes** to display the Response Time chart as part of the report. The default is Yes.
Units for Response Time report	Select the response time unit, msec or sec. The default is msec.
Threshold on Response Time chart (selected units)	Specify the response time threshold to display on the chart in the report. The default is 0, which suppresses the threshold indicator in the chart.
Select chart style	Click **Browse [...]** to set the appearance of the chart. The same parameters are used in both the Availability and Response Time charts, if both are produced. The default is Ribbon.
Select output folder	Select **Browse [...]** to specify the report filename and the report folder. You can specify a specific folder or have the system generate the folder each time the report runs.
Add job ID to output folder name?	Select **Yes** to add a job ID to the output folder name. Use a job ID to correlate a specific instance of a Report Script with the corresponding report. The default is unselected.
Index-Report Title	Select **Browse [...]** to configure report title settings and custom fields.
Add timestamp to title?	Select **Yes** to add a timestamp to the report title, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is unselected.
Event Notification	
Generate event on success?	Select **Yes** to raise an event when a report is generated. The default is Yes.
Severity level for report success	Set the event severity level to indicate the importance of an event in which the report is generated successfully. The default is 35.
Severity level for report with no data	Set the event severity level to indicate the importance of an event in which the report has no data. The default is 25.
Severity level for report failure	Set the event severity level to indicate the importance of an event in which the report cannot be generated. The default is 5.

Chapter 68
UNIX Knowledge Scripts

AppManager for UNIX provides the following Knowledge Scripts for monitoring UNIX servers.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AIXLparUtil	Monitors CPU utilization for Logical Partitions (LPAR) on AIX.
ApplicationProcessMonitor	Monitors the status of processes of an application.
AsciiLog	Monitors an ASCII text file for specific strings and messages logged.
CpuByProcess	Monitors CPU usage for each process and the total CPU usage for all processes.
CpuLoaded	Monitors CPU usage.
CpuResources	Monitors CPU consumption for users, the number of active processes, the number of threads, the number of context switches, and the number of interrupts per second.
CpuUtil	Monitors CPU utilization and queue length.
DNSConnectivity	Checks a DNS client's list of DNS servers to verify each DNS server is reachable and responding to client look-up requests.
DNSHealth	Checks memory and CPU usage for the DNS process and performs a basic `nslookup` test.
DNSReplication	Monitors replication between two name servers in a specified domain.
DynamicFileSystemSpace	Monitors used space and free space on only non-excluded mounted file systems and, optionally, checks for incremental increases in used space.
FailedLogon	Monitors failed logon and failed `su` attempts.
FileSystemSpace	Monitors used space and free space on mounted file systems and, optionally, checks for incremental increases in used space.
FileSystemSpaceLC	Uses a configuration file to monitor used space on mounted file systems and, optionally, checks for incremental increases in used space.
GeneralCounter	Monitors any user-specified system performance data.
HTTPHealth	Sends a status request to a Web server's HTTP port to check server operation.
LargeDir	Checks the disk space used by the directories you specify and the number of files under those directories.

Knowledge Script	What It Does
LogicalDiskBusy	Monitors logical disk operation time and the maximum queue length.
LogicalDiskIO	Monitors logical disk IO activity, including disk transfers, reads, and writes per second.
LogicalDiskUtilization	Monitors the utilization and I/O request queue for logical disk devices.
MemByProcess	Monitors the individual memory usage for each specified process and total memory usage for all specified processes.
MemShortage	Monitors the physical memory for a system.
MemUtil	Monitors physical memory, virtual memory, and paging files.
NetInterfacesCollision	Monitors network interface collision.
NetInterfacesConnectivity	Monitors the physical connection between network interface adapters and the network.
NetInterfacesDown	Checks the status of network interfaces.
NetInterfacesErrors	Monitors the percentage of input and output errors for network interfaces.
NetInterfacesIO	Monitors the input, output, and throughput of the network traffic on network interface cards.
PagingHigh	Monitors UNIX paging activity.
PhysicalDiskBusy	Monitors physical disk activity and response time.
PhysicalDiskIO	Monitors physical disk reads and writes in KB per second.
PingMachine	Checks server availability by running a Ping test and returning response time.
PortHealth	Checks whether system ports are working properly.
PrinterQueue	Monitors the printer queue length and the memory size of the documents in the queue.
PrivilegedProcs	Monitors the number of system processes with an effective user ID (euid) of `root`.
ProcessDown	Determines whether specified processes are currently running.
Processes	Monitors the total number of processes.
ProcessUp	Checks whether a specified process is running.
RemoteProcessDown	Monitors applications on remote UNIX computers using a proxy UNIX agent.
Report_CPULoad	Generates a detailed report about CPU usage and queue length.
Report_DiskUsageSummary	Generates a summary report about the percentage of disk space used and the amount of free space.
Report_MemoryUtilization	Generates a detailed report about the use of physical and virtual memory, and paging files.
Report_NetInterfacesIO	Generates a report about the use of bandwidth on network interface cards.
Report_SystemUpTime	Generates a report detailing the uptime and downtime (by percentage) of monitored computers.
Report_TopMemoryProcs	Generates a report about the total memory used by all processes and which processes consume the most memory resources.

Knowledge Script	What It Does
RunAwayProcs	Detects runaway processes by sampling CPU usage and (optionally) terminates processes.
RunCommand	Runs a non-interactive UNIX command.
SwapLow	Monitors the availability of swap areas.
Syslog	Monitors the `syslog` file for the search strings you specify.
SystemUpTime	Tracks the number of hours a computer has been operational since it was last rebooted.
TopCpuProcs	Monitors total CPU used by all processes and reports processes that consume the most CPU resources.
TopMemoryProcs	Monitors the total memory used by all processes and reports processes that consume the most memory.
ZombieProcs	Monitors the number of zombie processes.

Creating Filters with Regular Expressions

The AsciiLog, RemoteProcessDown, NT_UnixRemoteProcessDown, and Syslog Knowledge Scripts enable you to use regular expressions to define include and exclude filters for pattern-matching against the text being evaluated. Where available, include and exclude filters can be used independently or together to give you a great deal of control in looking for and filtering text files. You can also use the regular expression modifiers to further refine your filtering.

For example, if your **include filter** looks like this `replic.*` and you specify the modifier `i` to make the search case-insensitive, the regular expression contains the wildcard (`.`) and repeat (`*`) special characters, indicating you want to find strings that start with `replic` followed by any string of characters. Messages containing either `replication` or `replicated` are matched.

The format is the same for the exclude filter. For example, to find log entries that do not start with the string `success`, the exclude filter might look like this:

```
^success.*
```

If you are only searching for included strings, you can leave the exclude filter blank. If you want to retrieve all messages in the log in a given interval, you can specify `.*` for the include filter and leave the exclude filter blank.

Special Characters for Regular Expressions

The following special characters can be used in regular expressions:

Character	Purpose
.	Wildcard for any one character
*	Repeat zero or more occurrences
^	Beginning of the line
\$	End of the line
\	Escape the next meta-character
|	Alternate matches
[ ]	Any character in the class set. You can specify individual characters or ranges
( )	Grouping characters. For example, you can specify (a|b|c) to indicate a match with a, or b, or c.
+	Quantifier indicating one or more occurrences
?	Quantifier indicating zero or one occurrence
{*n*}	Quantifier indicating exactly *n* occurrence
\w	A word character (alphanumeric plus _)
\s	A white-space character
\d	A digit character

If you use any of these special characters in a literal string, you must "escape" it with a single backslash (\) character. For example, assume you're running the AsciiLog Knowledge Script, which scans an ASCII text file for specific strings and messages. Note that to search the log for the string **www.netiq.com**, the two periods in the string must be escaped to be included in the search string. Therefore, the literal string you would specify as a Knowledge Script parameter would be:

```
www\.netiq\.com
```

Modifiers for Regular Expressions

In addition to the special characters you can use in creating the regular expression, there are a number of modifiers that can be used to modify how pattern-matching is handled. Valid modifiers include

Modifier	Description
`c`	Complements the search list
`g`	Matches globally as many times as possible
`i`	Makes the search case-insensitive
`m`	Treats the string as multiple lines
`o`	Interpolates variables only once
`s`	Treats the regular expression string as a single long line
`x`	Allows for regular expression extensions

For additional information about writing regular expressions, see your Perl documentation.

AIXLparUtil

Use this Knowledge Script to monitor Logical Partitions (LPAR) utilization on AIX computers. LPAR utilization is measured in percentage. This Knowledge Script collects utilization data based on the following parameters:

- Percentage of partition utilized in user mode
- Percentage of partition utilized in system kernel mode
- Percentage of partition utilized for I/O operations
- Percentage of partition in idle mode
- Number of physical processesors consumed
- Entitled capacity consumed
- Logical processor utilization

You can set thresholds for each of these parameters. If the partition utilization exceeds any threshold, an event is generated.

Resource Object

CPU icon on AIX

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Number of seconds between samples	Enter the data collection interval, from 2 to 30, in seconds for the `lparstat` utility. The default value is 5 seconds.
Number of times lparstat should iterate before reporting an average value	Enter the iteration count, from 1 to 100, for the `lparstat` utility. The default value is 3.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Data Collection Options	
Collect data for %User CPU state? (y/n)	Set to **y** to collect data for the percentage of CPU used in user mode. By default, data is not collected.
Collect data for %System CPU state? (y/n)	Set to **y** to collect data for the percentage of CPU used in kernel/system mode. By default, data is not collected.
Collect data for %Wait CPU state? (y/n)	Set to **y** to collect data for the percentage of CPU used in I/O mode. By default, data is not collected.
Collect data for %Idle CPU state? (y/n)	Set to **y** to collect data for the percentage of CPU in the idle mode. By default, data is not collected.

Description	How to Set It
Collect data for total CPU utilization? (y/n)	Set to **y** to collect data for the total percentage of CPU used. This includes utilization data when the CPU is in user and kernel/system modes. By default, data is collected.
Collect data for number of physical processors consumed? (y/n)	Set to **y** to collect data for the number of physical processors consumed by the CPU. By default, data is collected.
Collect data for %Entitled capacity consumed? (y/n)	Set to **y** to collect data for the total percentage of entitled capacity used. By default, data is collected.
Collect data for %Logical processor utilization? (y/n)	Set to **y** to collect data for the total percentage of logical processor used. By default, data is collected.
Thresholds and Eventing	
Threshold -- Maximum %User CPU state. -1 disables	Enter the threshold value, between 1 and 100, for the maximum percentage of CPU utilization in user mode. An event is raised if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 90%.
Threshold -- Maximum %System CPU state. -1 disables	Enter the threshold value, between 1 and 100, for the maximum percentage of CPU utilization in the kernel/system mode. An event is raised if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 90%.
Threshold -- Maximum %Wait CPU state. -1 disables	Enter the threshold value, between 1 and 100, for the maximum percentage of CPU utilization in the I/O wait mode. An event is raised if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 90%.
Threshold -- Maximum %Idle CPU state. -1 disables	Enter the threshold value, between 1 and 100, for the maximum percentage of CPU in the idle mode. An event is raised if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 10%.
Threshold -- Maximum Total CPU utilization	Enter the threshold value, between 1 and 100, for the maximum percentage of total CPU utilization (in user and kernel/system modes). An event is raised if the CPU utilization exceeds this threshold. The default is 90%.
Threshold -- Maximum number of physical processors consumed. -1 disables	Enter the threshold value, between 1 and 100, for the maximum percentage of of number of physical processors consumed. An event is raised if the number exceeds this threshold. Enter -1 to disable the threshold. The default is disabled.
Threshold -- Maximum Total %Entitled capacity consumed. -1 disables	Enter the threshold value, between 1 and 1000, for the maximum percentage of of entitled capacity utilization. An event is raised if the capacity exceeds this threshold. Enter -1 to disable the threshold. The default is disabled.
Threshold -- Maximum %Logical processor utilization. -1 disables	Enter the threshold value, between 1 and 1000, for the maximum percentage of of logical processor utilization. An event is raised if the processor utilization exceeds this threshold. Enter -1 to disable the threshold. The default is disabled.

ApplicationProcessMonitor

Use this Knowledge Script to monitor the number of application processes for a particular application.

An application can include multiple application processes. Each application process in turn can have more than one process instance. If the total number of process instances for one of the application processes detected falls below the threshold count you set, an event is raised.

The threshold parameter allows you to set a separate threshold for multiple monitored processes. First, supply a list of processes to monitor for the **Process names** parameter. Separate the process names in the list with commas and no spaces. Then supply a comma-separated list of threshold values that correspond to the processes and are listed in the same order.

You also have the option to restart any process that appears to be down. Anytime the number of process instances for a process reaches 0, this Knowledge Script can invoke a restart command that you supply (see the **Command to restart processes with count of 0** parameter, below). You can enable events to notify you if the attempt to restart a process with a process count of 0 has succeeded or failed. These events are triggered by the output term corresponding to success in your command script. You need to supply this output term for the **Word(s) in restart command output that indicate success** parameter.

If you enable data collection, this Knowledge Script returns the current process instance count for all the processes in the monitored application(s).

Resource Object

UNIX CPU folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Application to monitor	Supply the name of the application whose processes you want to monitor. The default is `My Application`.
Process Monitoring	
Process names (comma-separated)	Supply the names of processes to monitor. Separate names of multiple processes with commas (,) and no spaces.
Threshold -- Minimum number of processes (comma-separated)	Specify the minimum number of process instances that must be running for each monitored process to prevent an event from being raised. Separate multiple threshold values with commas and no spaces. To ensure that the proper threshold is applied to the intended process, list thresholds in the same order as you listed processes for the **Process names** threshold.

Description	How to Set It
Threshold -- Maximum number of processes (comma-separated)	Specify the maximum number of process instances that must be running for each monitored process to prevent an event from being raised. If an application is running more than this number of process instances, an event will be raised. Separate multiple threshold values with commas and no spaces. To ensure that the proper threshold is applied to the intended process, list thresholds in the same order as you listed processes for the **Process names** threshold.
Command to restart processes with count of 0 (comma-separated)	Specify a command to use to restart any process whose process instance count is 0. Separate multiple commands with commas and no spaces. Leave this parameter blank if you do not want to restart processes automatically.
Word(s) in restart command output that indicate success (vertical bar-separated)	Specify a list of the words that will be returned by the scripts you supplied to indicate that the scripts succeeded in restarting a process. The presence of these words triggers the success event in AppManager. Use a vertical bar character (|) to separate multiple words, and use a comma (,) to separate the word groups for each process. The default is: `started|success|succeed`
Event Notification	
Raise event if number of processes falls below threshold?	Select **Yes** to raise an event if the process instance count for any monitored process falls below a threshold you set. The default is y.
Event severity when number of processes falls below threshold	Enter the event severity level, from 1 to 19, to indicate the importance of the event. The default is 10.
Event severity when attempt to restart process fails	Enter the event severity level, from 1 to 9, to indicate the importance of the event. The default is 5.
Event severity when attempt to restart process succeeds	Enter the event severity level, from 20 to 40, to indicate the importance of the event. The values you enter for the **Word(s) in restart command output that indicate success** parameter trigger this event. The default is 25.
Data Collection	
Collect data for number of processes?	Select Yes to collect data for charts and reports. If enabled, this script returns the number of process instances detected for each monitored process.

AsciiLog

Use this Knowledge Script to monitor an ASCII text file for specific strings and messages logged since the last monitoring interval. This Knowledge Script allows you to specify the filename, and a regular expression to identify the string to look for or to exclude. The script scans the ASCII file and reports the matching entries found since the last monitoring period. The script checks for changes to the text file that match the expression you enter; it does not re-scan the entire file at each interval unless it determines that the entire file is new (either because the new file size is smaller or because the cyclic redundancy check indicates there is a new file).

This Knowledge Script reads the entire file to find matching strings the first time it executes. AsciiLog tracks the last item read in the file persistently. If the Knowledge Script restarts, it is treated as the first iteration. Because the file it is monitoring has already been read before, the first iteration (that is, after restart), will start reading the file from where the marker stopped before it restarted.

You can also configure the script to perform a cyclic redundancy check (CRC) on the file for the purpose of determining when a file has been replaced rather than appended. If the original has been replaced by a file of the same size or by a larger file, the CRC will expose that change and cause the script to parse the entire new file.

If the file is recreated between intervals and the file size is smaller than the previous version of the file, the script treats it as a new file and searches it from the beginning.

The script raises an event if the number of lines matching your search criteria exceeds the threshold you set, or if the file is missing.

Note
To specify the include and exclude patterns, you need to be familiar with Perl regular expressions. Some information is available in the topic "Creating Filters with Regular Expressions" on page 3842.

You can use this script to monitor any text file the UNIX agent has permission to read. If the UNIX agent runs under a specific username rather than `root`, you may want to check whether that user account has read permission for the files you want to monitor.

Resource Object

UNIX computer icon

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Select **y** to raise events for the ASCII log. The default is y.
Event if log missing? (y/n)	Select **y** to raise an event if the log is missing. The default is y.
Create event for each matching line? (y/n)	Select **y** to raise a new event for each line that meets the event criteris. The default is no event is created.

Description	How to Set It
Do you want to limit the number of matching lines returned? (y/n)	Select **y** to limit the number of lines from the log file matching the search criteria that should be returned from a single job iteration. If you're expecting to see lots of matches, it is a good idea to enable this limit. For jobs that may return a very large number of matches, Operator Console performance may be adversely affected. Use the following parameter to specify a limit.
Maximum number of matching lines to return	Enter the maximum number of lines from the log file matching the search criteria that should be returned from a single job iteration. This limit avoids a degradation in Operator Console performance in cases where many lines match the search criteria. To set a limit here, you must enable the previous parameter. The default is 500 lines.
Parse the log file the first time? (y/n)	Select **y** to parse the file for the strings you have identified the first time the script runs. Subsequent iterations of the script measure any differences between this version of the file and any subsequent versions. If you select **n**, the first iteration of the script reads the file and inserts a marker at the end. Subsequent iterations of the script then measure differences in the script from this point forward.
Collect data? (y/n)	Select **y** to collect data. The script returns the number of lines containing matching strings. The default is no data is collected.
File names to parse (full path, UNIX-like shell pattern matching notation and comma-separated)	Enter the full path to the file you want to monitor or a regular expression representing the file. You can enter multiple files, comma separated without spaces. An event is created when the file is not found, and when files matching the description are added or deleted since the previous job. For example: `/tmp/applog.log,/\/var\/log\/netlog[0-9]/` The UNIX agent must run as an account that has permission to read the file. If you restrict read access on files, you might need to change the account the UNIX agent uses. The default is `/etc/hosts`.
Regular expression specifying the include filter	Enter a regular expression, in Perl, to identify the pattern you want to look for in the text file being monitored. Strings matching the include filter pattern are returned. The default expression matches all strings. For more information about writing Perl regular expressions, see Creating Filters with Regular Expressions.
Optional file with regular expressions specifying the include filter	If you do not want to enter a regular expression in the `Regular expression specifying the include filter` parameter, specify the full path to a file containing the regular expression specifying the include filter.
Modifier for the regular expression include filter	Enter any modifier you want to use to change the behavior of the regular expression. For example, specifying **i** for this parameter makes the include filter case-insensitive.
Regular expression specifying the exclude filter	Enter a regular expression, in Perl, to identify the pattern you want to exclude from matching in the text file being monitored. Strings with the exclude filter pattern are not returned. Separate multiple commands with commas and no spaces. For information about writing Perl regular expressions, see Creating Filters with Regular Expressions.
Optional file with regular expressions specifying the exclude filter	If you do not want to enter a regular expression in the `Regular expression specifying the excluse filter` parameter, specify the full path to a file containing the regular expression specifying the exclude filter.

Description	How to Set It
Modifier for the regular expression exclude filter	Enter any modifier you want to use to change the behavior of the regular expression. For example, specifying **i** for this parameter makes the exclude filter case-insensitive.
Threshold for matching lines	Enter the number of times to detect a line that matches the search criteria before raising an event. The default is zero, which is the first instance exceeds the threshold and raises an event.
Validate previously scanned lines with CRC? (y/n)	Select **y** to perform a cyclic redundancy check on the log file. The default is y.
Maximum number of log files to keep	Enter the maximum number of log files that should be created when the Knowledge Script logs ASCII entries. The default is 10.
Event severity level...	Set the event severity level, from 1 to 40, to indicate the importance: • **...for threshold crossing**. The default is 5. • **...for all other errors**. The default is 10.

CpuByProcess

Use this Knowledge Script to monitor whether specific processes have exceeded CPU thresholds. The Knowledge Script monitors CPU usage for each named process, as well as the total CPU usage for all named processes.

To determine CPU usage, the Knowledge Script checks the percentage of processor time that the threads for each process used to execute instructions.

If a process is not found, the Knowledge Script raises an event and the event detail message indicates which process was not found.

Resource Object

UNIX CPU folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Comma-separated list of process names or regular expressions	Enter one or more process names or regular expressions, separated by commas and no spaces. For example: `qtest.d`. The default is `proc1,proc2`.
Enable regular expressions?	Select **Yes** to if you want to use regular expressions to specify individual processes. The default is No.
Create event for each specified process? (y/n)	Set to **y** to raise events for individual processes. By default is events are raised.
Collect data for each specified process? (y/n)	Set to **y** to collect data for charts, graphs, and reports for individual processes. The default is no data is collected for individual processes to generate charts, graphs, or reports.
Maximum CPU usage (%) for each specified process	Select a threshold for the maximum CPU usage for each process. You cannot enter negative values. The default is 60.
Create event for the sum of all specified processes? (y/n)	Set to **y** to raise events for all processes. The default is y.
Collect data on the sum of all specified processes? (y/n)	Set to **y** to collect data for charts, graphs, and reports for all processes you are monitoring. The default is no summation data is collected for charts, graphs, or reports.
Maximum CPU usage (%) for all specified processes together	Enter a threshold for maximum combined CPU usage for all processes you are monitoring. You cannot enter negative values. The default is 95.
Event severity level	Enter the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

Note
This Knowledge Script does not detect invalid process names. If you enter an invalid process name, the Knowledge Script assumes that the process is not running, and reports zero as the CPU result.

CpuLoaded

Use this Knowledge Script to monitor average CPU usage and average queue length to determine whether the CPU is overloaded. You can monitor the average usage on each processor or the average usage across all processors in a computer.

If both the CPU usage and CPU queue length thresholds are exceeded, the CPU is overloaded and an event is raised.

On some systems the CPU queue length does not rise easily and you might want to ignore the queue length. If you do not want to monitor the CPU queue length, set **Maximum number of processes in the queue threshold** to -1.

Resource Objects

CPU folder or any individual CPU icon (for multiprocessor systems).

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if CPU usage and queue are over thresholds?	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. When set to y, this script returns the average CPU utilization percentage (%) and the average CPU run queue length. The default is n. **Tip** If you only want to collect run queue length data, use the UNIX_GeneralCounter Knowledge Script.
Monitor overall CPU load? (y/n)	Set to **y** to monitor the average load across all processors in a computer. If you are collecting data, setting this option to **y** creates a single data stream for all processors. Set to **n** to monitor the average load for each processor separately. If you are collecting data, setting this option to **n** creates a separate data stream for each processor. The default is y. **Note** For a single CPU system, monitoring all CPUs produces the same results as monitoring an individual CPU.
Maximum CPU usage (%) threshold	Type a threshold for maximum CPU utilization (user plus kernel). The default is 90.
Maximum number of processes in the queue threshold	Type a queue length threshold. CPU queue length indicates how many processes are ready to run. The default is 2. If you do not want to monitor the CPU queue length, set the threshold to -1.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Example of How this Script Is Used

This script monitors both the percentage of CPU used and processor queue length because, by itself, high CPU usage may not indicate a problem. Instead, you need to consider several factors, including:

- Queue length (Load average)
- How you are using the computers monitored
- Your overall strategy for the environment

For example, if you have a **transactional** environment on a computer consistently using 90% of the CPU, the computer is full. However, if the queue length remains low and stable (for example, never more than 2 processes waiting), it might indicate the computer is sized perfectly for maximum efficiency. If the queue length increases and you have processes waiting, it is likely to be a problem you need to address.

In a **batch** environment, consider setting the thresholds differently; for example, during down times when batch jobs are not running you might want an event if CPU usage is over 50% and any process is waiting (queue length at 0) to ensure the computer has enough CPU headroom when the batch jobs are running.

Other factors to consider are long-range plans, such as the number of users you expect to support, for how long, and how much room for growth you need. For example, you may want to set the CPU usage lower to give you an early warning that you need to off-load some processing or order new systems.

Selecting Overall or Individual CPU Load

Monitoring load for each CPU individually provides more specific information about what is happening on a system. For example, if you monitor average load and see CPU usage is 100%, it does not tell you as much about the resource usage as seeing that CPU 0 is running at 90% and CPU 1 is running at 10%.

Handling Spikes

Because CPU and queue length are often subject to temporary spikes, you shoul set a short interval, such as every 3 to 5 minutes, but raise an event only after thresholds are exceeded in 3 consecutive periods.

Collecting Data

This Knowledge Script is typically used to raise events, but if you collect data, you can use the information to identifying usage trends. For example, seeing the CPU usage growing steadily, can help you plan for growth. If you want to do this type of analysis, consider running a second job at a less frequent interval.

You can configure this Knowledge Script to collect data on the average CPU utilization percentage (%) and the average CPU run queue length. You can collect data for the average usage on each processor or the average usage across all processors in a computer.

Working with Multi-Processor Systems

On a multi-processor system, the total CPU utilization is the average percentage of time that all the processors on the system are busy executing non-idle threads. For example:

- if all processors are always busy, this is 100%.
- if all processors are 50% busy, this is 50%.
- if 25% of the processors are busy and all processors use a single queue in which threads wait for a processor cycle, this is 25%.

CpuResources

Use this Knowledge Script to monitor CPU resource consumption for users. This Knowledge Script also monitors the number of active processes, the number of threads, the number of context switches per second, and the number of interrupts per second. If any metric exceeds one of the thresholds you set, an event is raised.

Resource Object

CPU folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data for...	Set to **y** for any of these parameters to collect the corresponding data for graphs and reports. • **... user CPU time** to return the percentage of user CPU time usage for the interval. • **... number of processes** to return the number of active processes for the interval. • **... number of threads** to return the number of threads for the interval. • **... context switches per second** to return the number of context switches per second for the interval. • **... interrupts per second** to return the number of interrupts per second for the interval. By default, data is not collected.
Event if...	Set to **y** to raise events if the corresponding threshold is crossed. The default is y. • **... user CPU time (%) exceeds threshold**. Raises an event if user CPU time usage exceeds the threshold in the interval. • **... number of processes exceeds the threshold**. Raises an event if the number of active processes exceeds the threshold in the interval. • **... number of threads exceeds the threshold**. Raises an event if the number of threads exceeds the threshold in the interval. • **... context switch rate exceeds the threshold**. Raises an event if the number of context switches per second over the threshold in the interval. • **... interrupt rate exceeds the threshold**. Raises an event if the number of interrupts per second exceeds the threshold in the interval.

Description	How to Set It
Threshold -- Maximum...	Set the thresholds for the monitoring you want to do. • **... CPU usage (%) for user time**. Enter a threshold for the maximum CPU usage in user mode. The default is 80%. • **... number of processes**. Enter a threshold for the maximum number of processes that can be running simultaneously. The default is 100 processes. • **... number of threads**. Enter a threshold for the maximum number of threads that can be running simultaneously. The default is 400 threads. • **... context switch rate**. Enter a threshold for the maximum number of context switches per second. The default is 100 switches per second. • **... interrupt rate**. Enter a threshold for the number of interrupts per second. The default is 500 interrupts per second.
Event severity...	Set the event severity level, from 1 to 40, to indicate the importance of each event. • **...for miscellaneous runtime errors**. The default is 8. • **...when user CPU time exceeds threshold**. The default is 5. • **...when number of processes exceeds threshold**. The default is 5. • **...when number of threads exceeds threshold**. The default is 5. • **...when context switch rate exceeds threshold**. The default is 5. • **...when interrupt rate exceeds threshold**. The default is 5.

CpuUtil

Use this Knowledge Script to monitor CPU utilization and queue length. CPU utilization is measured in percentage. This Knowledge Script collects utilization data based on the following parameters:

- User: Percentage of CPU utilized in user mode
- System: Percentage of CPU utilized in kernel mode
- Wait: Percentage of CPU utilized for I/O operations
- Idle: Percentage of CPU in idle mode

You can set thresholds for each of these parameters. If the CPU utilization exceeds any threshold, an event is generated.

If you are using Logical Partitions (LPAR) on AIX, use the AIXLparUtil Knowledge Script.

Resource Object

CPU icon

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitor overall CPU load? (y/n)	Set to **y** to monitor the total load on the CPU. If you set the value to **n**, only individual CPUs are monitored By default, CPU load is monitored.
Number of seconds between samples	Enter the data collection interval (in seconds) for the `sar` utility. The default value is 5 seconds.
Number of times sar should iterate before reporting an average value	Enter the iteration count for the `sar` utility. The default value is 1.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Data Collection Options	
Collect data for %User CPU state? (y/n)	Set to **y** to collect data for the percentage of CPU utilized in user mode. By default, data is not collected.
Collect data for %System CPU state? (y/n)	Set to **y** to collect data for the percentage of CPU utilized in kernel/system mode. By default, data is not collected.
Collect data for %Wait CPU state? (y/n)	Set to **y** to collect data for the percentage of CPU utilized in I/O mode. By default, data is not collected.
Collect data for %Idle CPU state? (y/n)	Set to **y** to collect data for the percentage of CPU in the idle mode. By default, data is not collected.
Collect data for Total CPU utilization? (y/n)	Set to **y** to collect data for the total percentage of CPU utilized. This includes utilization data when the CPU is in user and kernel/system modes. By default, data is collected.

Description	How to Set It
Collect data on CPU Queue Length? (y/n)	Set to **y** to collect data for the number of processes in the CPU run queue. By default, data is not collected.
Thresholds and Eventing	
Event if CPU usage exceeds thresholds? (y/n)	Set to **y** to raise an event when the CPU usage exceeds the thresholds you have specified. By default, events are raised.
Threshold -- Maximum %User CPU state. -1 disables	Enter the threshold value, between 1 and 100, for the maximum percentage of CPU utilization in user mode. An event is raised if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 90%.
Threshold -- Maximum %System CPU state. -1 disables	Enter the threshold value, between 1 and 100, for the maximum percentage of CPU utilization in the kernel/system mode. An event is raised if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 90%.
Threshold -- Maximum %Wait CPU state. -1 disables	Enter the threshold value, between 1 and 100, for the maximum percentage of CPU utilization in the I/O wait mode. An event is raised if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 90%.
Threshold -- Maximum %Idle CPU state. -1 disables	Enter the threshold value, between 1 and 100, for the maximum percentage of CPU in the idle mode. An event is raised if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 10%.
Threshold -- Maximum Total CPU utilization	Enter the threshold value, between 1 and 100, for the maximum percentage of total CPU utilization (in user and kernel/system modes). An event is raised if the CPU utilization exceeds this threshold. The default is 90%.
Maximum number of processes in the queue threshold	Enter the maximum number of processes that should be allowed to be queued. If the number of processes in queue exceeds the threshold, an event is raised. By default, events are not raised.
Event if queue length is over threshold? (y/n)	Set to **y** to raise an event when the queue length exceeds the threshold you have specified. By default, events are not raised.

DNSConnectivity

Use this Knowledge Script to check a DNS client's list of name servers. The Knowledge Script identifies the servers to check by scanning the `/etc/resolv.conf` file, then verifies that each server is reachable with a `ping` command and responds to an `nslookup` request. You should run this Knowledge Script on one or more DNS clients to ensure your DNS servers are available and responding to address (`nslookup`) requests. If any server listed in `/etc/resolv.conf` fails to reply to the `ping` command or the `nslookup` request, an event is raised.

You can only use this Knowledge Script on computers that are running a DNS server.

Note
If your firewall configuration is set to disable the ping command, you should disable the Attempt to ping servers parameter to avoid unwanted events.

Resource Object

Network folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Attempt to ping server? (y/n)	Set to **y** to monitor the availability of DNS servers by sending a `ping` command. Set to n if you do not want to verify the server availability using a `ping` command. For example, if your organization or firewall configuration is set to disable the `ping` command, you should set this option to n to avoid unwanted events. The default is y.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

DNSHealth

Use this Knowledge Script to check the health of the DNS server by monitoring memory and CPU usage for the DNS process and attempting a basic address look-up (`nslookup`) request. With this Knowledge Script, you can set separate thresholds for the maximum percentage of CPU and memory the DNS process should be using.

This script will raise an event if:

- CPU used by the DNS process exceeds the threshold
- Memory used by the DNS process exceeds the threshold
- The DNS process fails to respond to the look-up request

Because temporary spikes or increases in memory or CPU consumption are typically of less concern than look-up failures, the default event severity level signalling that the memory or CPU threshold has been crossed is a Warning event. For look-up failures, the default severity level indicates that the failure is a Severe event.

You can only use this Knowledge Script on computers that are running a DNS server.

Resource Object

Network folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if...	Set to **y** to raise events if the corresponding threshold is crossed or operation failed. • **... CPU usage is over the threshold** to raise an event for CPU usage over the threshold in the interval. The default is y. • **... memory usage is over the threshold** to raise an event for memory usage over the threshold in the interval. The default is y. • **... bind is not running or nslookup fails** to raise an event if the DNS process is down or the look-up request fails in the interval. The default is y.
Collect cpu usage data? (y/n)	Set to **y** to collect CPU data for charts and reports. If set to y, the script returns the average percentage of CPU used. The default is n.
Collect memory usage data? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the average percentage of memory the DNS process used. The default is n.
Maximum CPU usage (%) threshold	Enter a threshold for maximum percentage of CPU the DNS process should be allowed to use before raising an event. The default is 90% of available CPU.
Maximum memory usage (%) threshold	Enter a threshold for maximum percentage of memory the DNS process should be allowed to use before raising an event. The default is 50% of available memory.

Description	How to Set It
Site name to look for using nslookup	Enter the name of the site you want the DNS server to look for using `nslookup`.
Event severity when...	Set the event severity level, from 1 to 40, to indicate the importance of each event. • **... CPU usage (%) over the threshold**. The default is 15. • **... memory usage (%) over the threshold**. The default is 15. • **... DNS is down or nslookup fails**. The default is 5.

DNSReplication

Use this Knowledge Script to monitor replication between primary and backup DNS nameservers. This Knowledge Script queries the Start of Authority (SOA) records for the DNS server on the local computer where you run the job and the remote DNS server you specify to determine the serial number that's currently in the SOA record for each server. This serial number is incremented when there are changes to the DNS zone. If the serial numbers are the same, there is full replication of the primary DNS server's address list. By default, if the serial numbers are not exactly the same in the SOA records (that is, the maximum serial number difference threshold is set to zero), an event is raised.

Although full replication is desirable in most cases, you can specify a threshold for the serial number difference that you deem acceptable for your organization. For example, you may find it acceptable for the serial numbers on backup DNS servers to be out of sync periodically and so may want to adjust the maximum serial number difference threshold to a higher value to allow for this. If the difference between the serial number on the computer where you run the job and the remote DNS server you specify exceeds the acceptable threshold, an event is raised.

You can only use this Knowledge Script on computers that are running a DNS server.

Note
Both the DNS server where you run the job and the DNS server you specify in this Knowledge Script should be nameservers responsible for the domain you specify in this Knowledge Script.

Resource Object

Network folder

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events if the difference between the serial numbers in the SOA records is over the threshold. The default is y.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the SOA serial number difference between the servers. The default is y.
Maximum serial number difference	Enter a threshold for the maximum difference between SOA serial numbers. The default is 0 (identical serial numbers).
Remote DNS server to compare local SOA records against	Enter the name of the DNS server you want to compare SOA records against. The computer you specify should be a backup or secondary DNS server in the same domain as the DNS server where you drop the Knowledge Script job.

Description	How to Set It
Domain name	Enter the name of the domain the local and remote DNS nameservers are responsible for serving.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity is 25, indicating this is an “informational” event that does not require immediate attention. If DNS replication is critical in your environment, you may want to set the event severity higher, for example 1-10, for greater visibility.

DynamicFileSystemSpace

Use this Knowledge Script to monitor the used space and free space on various types of mounted file systems, including NFS mounted file systems, that are often unmounted then mounted again. You can also check for incremental increases in used space beyond the specified threshold. For example, you can configure this Knowledge Script to **Create a new event for incremental increases** and set the **Threshold for incremental increases** to 5% to create an event when used space exceeds 80%, and create a new event when used space exceeds 85%, 90%, and 95%.

When checking for incremental increases, a single event is created if the specified threshold is met; event collapsing is not applicable. If you want to monitor incremental increases in used space, do NOT enable the event option on the **Advanced** tab to **Generate a new event when original event condition no longer exists**. If you enable this option, the Knowledge Script incorrectly raises an event.

Resource Object

Logical disk or disks

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if threshold exceeded?	Specify whether you want to raise an event if the amount of file system space used or free exceeds the capacity threshold you specify. The default is y.
Threshold -- Maximum used space	Type a threshold for the maximum amount of used space (total capacity). If you use this parameter, select the units you want to use. The default is 80.
Threshold -- Minimum free space	Type a threshold for the minimum amount of free space available (total capacity) for use. If you use this parameter, select the units you want to use. The default is -1, meaning no minimum.
Units	Select the unit of measure you want to use to determine the threshold for the used space and free space parameters. Available units are percentage, kilobytes, and megabytes. The default is percentage.
Incremental Event Notification	
Raise new event for incremental increases?	Specify whether you want to continue to raise events if the amount of file system space used exceeds the capacity threshold you specify and continues to increase since the previous event. The default is n.
Threshold -- Incremental increases	Type the amount that must be exceeded before another event is raised while the initial threshold remains exceeded. The default is 0.
Data Collection	
Collect data for used and available space?	Specify whether you want to collect data for charts, graphs, and reports. When set to y, this script returns the percentage of used file system space, the amount of available file system space, the used space, and free space. By default, this script does not collect data.

Description	How to Set It
Event severity when used space exceeds threshold	Set the event severity level, from 1 through 40, to indicate the importance of the event. The default is 5.
Filesystem types to exclude	Specify the types of file systems you do not want to monitor. To determine the type of your mounted file system, use the `df` command with the `-T` option. Separate the file system types by a comma without a space. The default is: `subfs,usbfs,proc,iso9660,fd,ctfs,mntfs,objfs,devfs`

FailedLogon

Use this Knowledge Script to monitor the number of failed log-on and switch-user-to-root (`su`) attempts since the last interval. The result is always zero for the first interval so that the Knowledge Script can establish a baseline for subsequent checks. A higher than average number of failed logon or `su` attempts may indicate an attempt to break in to the server or that password guessing programs are being used to try to crack the security on the server.

If the number of failed logon or switch user attempts exceeds the threshold you set, an event is raised.

Resource Object

UNIX computer icon

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event for...	Set to **y** to raise events if the threshold is crossed or operation failed. • **... failed login** to raise an event if the number of failed user login attempts exceeds the threshold in the interval. On Solaris, a failed log-on attempt is only registered after five consecutive failures. The default is y. • **... failed su** to raise an event if the number of failed attempts to log in as root using the (`su`) command exceeds the threshold in the interval. The default is y.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the number of failed login attempts for the interval. The default is n.
System log file (leave blank for default)	Type the full path to the location of the log file that records failed attempts to use the `login` command. For more information about how to register logins and record failed attempts to a log file, see your operating system documentation. If you leave this parameter blank, the script checks for the log file in the following default locations: • On Sun Solaris, the default location is `/var/adm/loginlog` • On HP-UX 11.1 and earlier, the default location is `/var/adm/btmp` • On HP-UX 11.2 and later, the default location is `/var/adm/btmps` • On IBM AIX, the default location is `/etc/security/failedlogin` • On Linux, the default location is `/var/log/messages` **Note:** On IBM AIX computers, if you configured syslog to log failed login attempts in a file other than the default file, ensure the non-default log file is available by performing the following steps: 1. Create the log file where you want to log failed login attempts. For example, `/var/adm/messages`. For more information, see your IBM AIX documentation. 2. Specify the full path to the log file in the `syslog.conf` system file. 3. Restart `syslog` for the changes to take effect.

Description	How to Set It
System su log file (leave blank for default)	Type the full path to the location of the system log file that records failed attempts to use the `su` command. For more information about how to log failed su attempts to a log file, see your operating system documentation. If you leave this parameter blank, the script checks for the log file in the following default locations: • On Sun Solaris, the default location is `/var/adm/sulog` • On HP-UX, the default location is `/var/adm/sulog` • On IBM AIX, the default location is `/var/adm/sulog` • On Linux, the default location is `/var/log/messages` **Note:** On IBM AIX computers, if you configured syslog to log failed attempts to use the `su` command in a file other than the default file, ensure the non-default log file is available by performing the following steps: 1. Create the log file where you want to log failed attempts to use the `su` command. For example, `/var/adm/sulog`. For more information, see your IBM AIX documentation. 2. Specify the full path to the log file in the `syslog.conf` system file. 3. Restart `syslog` for the changes to take effect.
Maximum number of failed login attempts	Enter a threshold for the number of failed logon attempts. The default is 1 failed attempt. **Tip** If you find you are generating too many “insignificant” events from users entering passwords incorrectly, you may want to determine a “typical” log on failure pattern (for example 5 per 24 hours) using the Collect data option, then set this parameter based on the typical pattern.
Maximum number of failed `su` attempts	Enter a threshold for the number of failed `su` attempts. The default is 1 failed attempt.
Event severity level...	Set the event severity level, from 1 to 40, to indicate the importance of each event. • **... for failed login**. The default is 8. • **... for failed su**. The default is 8.

FileSystemSpace

Use this Knowledge Script to monitor the used space and free space on mounted file systems and optionally, check for incremental increases in used space beyond the specified threshold.

For example, you can configure this Knowledge Script to **Create a new event for incremental increases** and set the **Threshold for incremental increases** to 5% to create an event when used space exceeds 80%, and create a new event when used space exceeds 85%, 90%, and 95%.

When checking for incremental increases, a single event is created if the specified threshold is met; event collapsing is not applicable. If you want to monitor incremental increases in used space, do NOT enable the event option on the **Advanced** tab to **Generate a new event when original event condition no longer exists**. If you enable this option, the Knowledge Script incorrectly raises an event.

If you want to prevent monitoring of some types of file systems, use the DynamicFileSystemSpace Knowledge Script.

Resource Objects

Any logical disk or disks.

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if threshold exceeded?	Specify whether you want to raise an event if the amount of file system space used or free exceeds the capacity threshold you specify. The default is y.
Threshold -- Maximum used space	Type a threshold for the maximum amount of used space (total capacity). If you use this parameter, also select the units you want to use. The default is 80.
Threshold -- Minimum free space	Type a threshold for the minimum amount of free space available (total capacity) for use. If you use this parameter, also select the units you want to use. The default is -1, meaning no minimum.
Units	Select the unit of measure you want to use to determine the threshold for the used space and free space parameters. Available units are percentage, kilobytes, and megabytes. The default is percent.
Incremental Event Notification	
Raise new event for incremental increases?	Specify whether you want to continue to raise events if the amount of file system space used exceeds the capacity threshold you specify and continues to increase since the previous event. The default is n.

Description	How to Set It
Threshold -- Incremental increases	Type the amount that must be exceeded before another event is raised while the initial threshold remains exceeded. The default is 0.
Data Collection	
Collect data for used and available space?	Specify whether you want to collect data for charts, graphs, and reports. When set to y, this script returns the amount of used file system space, the amount of available file system space, the used space, and free space. By default, this script does not collect data.
Event severity when used space exceeds threshold	Set the event severity level, from 1 through 40, to indicate the importance of the event. The default is 5.

FileSystemSpaceLC

This Knowledge Script uses a configuration file on the managed client computer to monitor the percentage of used space on mounted file systems as reported by the system `df` command and optionally, check for incremental increases in used space beyond the specified threshold. Using the configuration file, you can specify a different threshold for each file system and therefore receive event information for each (for example, when `/usr` is at 95% and `/bin` is at 80%).

When checking for incremental increases, a single event is created if the specified threshold is met; event collapsing is not applicable. If you want to monitor incremental increases in used space, do NOT enable the event option on the **Advanced** Knowledge Script Properties tab to **Generate a new event when original event condition no longer exists**. If you enable this option, the Knowledge Script incorrectly creates an event.

Note
You can set thresholds for file systems not in the configuration file but found as the result of a df command. You can enable events and data collection for these file systems. You can also use this Knowledge Script to dynamically monitor file systems without re-running discovery.

Resource Object

Any logical disk folder

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Default Event Thresholds for Mounted File Systems	
Event Notification	
Raise event if threshold exceededfor a mounted file system?	Specify whether you want to raise an event if the percentage of file system space used exceeds the default used threshold you specify for mounted file systems. The default is n.
Threshold -- Maximum used space	Type a threshold for the maximum percentage of file system space available (total capacity) that should be in use by mounted file systems. The default is 80.
Incremental Event Notification	
Raise new event for incremental increases?	Specify whether you want to continue to raise events if the percentage of file system space used exceeds the capacity threshold you specify and continues to increase since the previous event. The default is n.
Threshold -- Incremental increases	Type the percentage that must be exceeded before another event is raised while the initial threshold remains exceeded. The default is 5.
Event severity when threshold exceeded	Set the event severity level, from 1 through 40, to indicate the importance of the event. The default is 5.

Description	How to Set It
Default Data Collection Options for Mounted File Systems	
Collect data for space usage on unspecified file systems?	Specify whether you want to collect data for charts, graphs, and reports for mounted file systems. When set to y, this script returns the percentage of used file system space, the percentage of available file system space, the used space (MB), and free space (MB). By default, this script does not collect data.
Monitoring	
File system types to exclude	Specify the types of systems you do not want to monitor, separated by commas with no space. The default is `subfs,usbfs,proc,iso9660,fd`.
Monitor mounted NFS shares?	Specify whether you want to monitor mounted Network File Systems. The default is n.

Override configuration file (full path) (optional)	Type the full path to the logical configuration file you created. The default is `/etc/NQfs.conf`.
	Use the following format for the configuration file; enter one line per entry:
	`"doevent?,dodata?,threshold,mountpoint"`
	`y,n,80,/usr`
	`n,n,75,/var`
	`y,y,90,/tmp`

GeneralCounter

Use this Knowledge Script to monitor system performance. This script maps elements of UNIX performance data to use a format similar to Windows Performance Monitor counters using the Object, Counter, Instance model, and identifies which of those UNIX "counters" you want to monitor. Information for the objects and counters you specify is returned to the management server. The performance data is then stored in the AppManager repository and available for reporting in AppManager charts and reports.

There are several base objects, such as:

- UX Disk
- UX Virtual Memory
- UX Processor
- UX Block IO
- UX Networking
- UX Paging
- UX Swapping

Each object has multiple counters and can have multiple instances. You can set both high (Over) and low (Under) thresholds for the counter you are monitoring, and can set up the script to raise an event if the value of the counter you select is greater than the **Maximum threshold** value, or is less than the **Minimum threshold** value. You can also specify a consecutive number of times that the over or under threshold value must be crossed before an event is raised.

Note
An event is raised only if the counter value is greater than the specified Maximum threshold value or is less than the specified Minimum threshold value. If a counter does not exist on the managed client, the Knowledge Script terminates with an error.

Resource Object

UNIX computer icon

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data for current counter value? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the current value of the specified counter. The default is n.
Raise event if maximum threshold is exceeded? (y/n)	Set to **y** to raise an event if the counter value is greater than the value specified in as the **Maximum threshold** parameter. The default is y.

Description	How to Set It
Threshold -- Maximum counter value	Enter a greater-than threshold for the counter value. If the counter you are monitoring exceeds this value, an event is raised if the **Raise event if maximum threshold is exceeded?** parameter is enabled. The default is 500. **Tip** Keep in mind that the units this value represents (for example, a number, percentage, or rate) depend on the specific counter you are monitoring.
Raise event if minimum threshold is not met? (y/n)	Set to **y** to raise an event if the counter value is less than the value specified in the **Minimum threshold** parameter. The default is y.
Threshold -- Minimum counter value	Enter a lower-limit threshold for the counter value. If the counter you are monitoring falls below this value, an event is raised if the **Raise event when minimum threshold not met?** parameter is enabled. The units this value represents depend on the specific counter you are monitoring. The default is 20.

Counter to monitor	Type the object, counter, and instance(s) to monitor.
	Use the format *object*|*counter*|*instance*. For example:
	`UX Processor|%System Time|_Total`
	The names are case-sensitive and the delimiter (|) is required. You can enter up to 5 counters, separated by commas and no spaces.
	Some counters require you to specify an instance name as well as the object and counter. In most cases, if a counter requires an instance name, you can specify the specific instance, for example, a specific CPU or device name, or `_Total` for all instances.
	Alternatively, you can leave the instance blank to indicate `_Total` instances. For example:
	`UX Block IO|Reads/s|,UX Block IO|Writes/s|`
	If instances are not applicable for a counter, you can leave the instance blank. For example:
	UX Swapping|Swap in KBytes/s|

Consecutive times threshold exceeded	Enter the number of consecutive times the maximum or minimum threshold should be exceeded before an event is raised. The default is 1 time.
Event severity when...	Set the event severity level, from 1 to 40, to indicate the importance of each event. By default, the severity levels are: • Maximum threshold--5 • Minimum threshold--8 • No counter/instance found--15

Examples of How this Script Is Used

Use this Knowledge Script to yield performance information for the counters you are interested in monitoring. If is particularly useful for monitoring system statistics not already covered with other Knowledge Scripts and customizing the monitoring of your UNIX servers. With AppManager for UNIX, you can use the counter data to start corrective actions when thresholds are crossed, generate more complex and sophisticated graphs, and provide historical information for reporting, trend analysis, and capacity planning.

When specifying counters, use the format *object*|*counter*|*instance*. For example:

```
UX Processor|%System Time|_Total
```

Object and counter names are case-sensitive and the delimiter (|) is required.

HTTPHealth

Use this Knowledge Script to check the operation of an HTTP server. This Knowledge Script connects to the Web servers you specify and sends a status request. If the Web server does not respond to the request, an event is raised.

Resource Object

UNIX computer icon

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is n.
Web server address list (separated by commas and no spaces)	Enter a list of Web server addresses, separated by commas, that you want to check. You can specify the address by hostname, IP address, or fully qualified domain name. For example: `Apache3,64.220.16.1,ajax.com.local`
Event severity level	Set the event notification level, from 1 to 40, to indicate the importance of the event. The default severity level is 8.

LargeDir

Use this Knowledge Script to monitor the directories you specify. The Knowledge Script checks the disk space used by the directories you specify and the number of files under those directories. You can set this Knowledge Script to check directories recursively or to only check in the directories you specify, and to raise an event when disk usage is over the threshold you set or when the number of files in a directory is over the threshold you set.

Resource Object

UNIX computer icon

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if disk space usage is over the threshold? (y/n)	Set to **y** to raise an event if the disk space used by any monitored directory exceeds the disk space threshold. The default is y.
Collect data on disk space usage? (y/n)	Set to **y** to collect data for charts and reports. The default is n.
Maximum disk space used threshold (in KB)	Type the maximum amount of disk space, in KB, that should be used for the directory. The default is 1000.
Event if the number of files is over the threshold? (y/n)	Set to **y** to raise an event if the number of files in any monitored directory exceeds the file threshold your set. The default is y.
Collect data on the number of files? (y/n)	Set to **y** to collect data for charts and reports. The default is n.
Maximum number of files threshold	Type the maximum number of files that should be contained in the directory. The default is 1000.
Event severity level	Set the event notification level, from 1 to 40, to indicate the importance of the event. The default severity level is 15.
Include sub-directories recursively (y/n) ?	Set to **y** to include disk usage and file information for all sub-directories recursively. The default is y.
List of directories to search (separated by commas)	Type the directory path you want to monitor. You can specify multiple directories, separated by commas. For example: `/usr/home,/usr/mail`. The default is `/tmp`.

LogicalDiskBusy

Use this Knowledge Script to monitor the logical disk activity on one or multiple disks. You can use this Knowledge Script to set a threshold for maximum disk operation time and the maximum queue length. This Knowledge Script raises an event if either the disk operation time or the queue length exceeds the threshold. This Knowledge Script only provides logical disk metrics that are provided by the operating system kernal.

Do not use this Knowledge Script to monitor queue length for a logical volume on VERITAS or AIX.

On Linux operating systems, this Knowledge Script:

- Does not work on kernel versions 2.6 or later
- Requires the optional sysstat package to be installed
- Does not monitor file-based file systems

Resource Objects

Any logical disk or disks on Solaris, Linux, or AIX.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold is exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data for disk operation time and queue length? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the percentage of logical disk and waiting queue in use. The default is n.
Threshold -- Maximum disk operation time	Enter a threshold for the maximum amount of time a disk operation should take. The default is 200 milliseconds.
Threshold -- Maximum I/O queue length	Enter a threshold for the maximum number of processes that should be in the I/O queue at any time. The default is 1.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

LogicalDiskIO

Use this Knowledge Script to monitor the logical disk input/output (I/O) activity. This Knowledge Script monitors the number of logical disk transfers, logical disk reads, and logical disk writes per second. You can set a threshold for each metric. If logical disk I/O exceeds any of the thresholds you set, an event is raised.

Resource Objects

Any logical disk or disks

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold is exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data for transfers per second? (y/n)	Set to **y** to collect data for graphs and reports. If enabled, returns the number of transfers per second for each logical disk. The default is n.
Collect data for reads per second? (y/n)	Set to **y** to collect data for graphs and reports. If enabled, returns the number of reads per second for each logical disk. The default is n.
Collect data for writes per second? (y/n)	Set to **y** to collect data for graphs and reports. If enabled, returns the number of writes per second for each logical disk. The default is n.
Threshold -- Maximum transfers per second	Enter the maximum number of transfers per second that can occur before an event is raised. The default is 80.
Threshold -- Maximum reads per second	Enter the maximum number of reads per second that can occur before an event is raised. The default is 50.
Threshold -- Maximum writes per second	Enter the maximum number of writes per second that can occur before an event is raised. The default is 50.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

LogicalDiskUtilization

Use this Knowledge Script to monitor the logical disk activity. This Knowledge Script raises an event if either the percentage of disk utilization or the percentage of time the I/O request queue is not empty exceeds the threshold.

Do not use this Knowledge Script to monitor:

- I/O queue utilization on AIX
- VERITAS logical volumes
- File-based file systems on HP-UX

On Linux operating systems, this Knowledge Script:

- Does not work on kernel versions 2.6 or later
- Requires the optional sysstat package to be installed

Resource Objects

Any logical disk or disks on Solaris, Linux, and AIX.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold is exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the percentage of logical disk and waiting queue in use. The default is n.
Threshold -- Maximum disk utilization	Enter a threshold for the maximum percentage of logical disk that should be in use. The default is 95%.
Threshold -- Maximum I/O queue utilization (Solaris only)	Enter a threshold for the maximum percentage of time processes should be waiting in the I/O queue. The default is 50%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

MemByProcess

Use this Knowledge Script to monitor memory usage for specified processes. The Knowledge Script monitors individual memory use for each specified process, and the total memory use for all specified processes. If a process is not found, the Knowledge Script assumes that the process is not currently running, and reports zero as the memory result.

If the memory use for any monitored process exceeds the threshold you set, an event is raised.

Note
This Knowledge Script does not detect invalid process names. If you enter an invalid process name, the Knowledge Script assumes that the process is not running, and reports zero as the result.

Resource Object

UNIX computer icon

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Comma-separated list of process names	Enter one or more process names, separated by commas and no spaces.
Create event for each specified process? (y/n)	Set to **y** to raise events when the memory usage is over the threshold for individual processes. The default is y.
Collect data for each specified process? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the memory usage for each process. The default is n.
Maximum memory usage (KB) for each specified process	Enter a maximum threshold for memory usage for each process. The default is 20000 KB.
Create event for the sum of all specified processes? (y/n)	Set to **y** to raise events when the combined memory usage for all specified processes is over the threshold. The default is y.
Collect data on the sum of all specified processes? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the combined memory usage for all specified processes. The default is n.
Maximum memory usage (KBs) for all specified processes together	Enter a threshold for combined memory usage for all processes you are monitoring. The default is 32000 KB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

MemShortage

Use this Knowledge Script to monitor the physical memory for a system. This Knowledge Script monitors the swapping scan rate to determine if more physical memory might help system performance. Any non-zero scan rate value can indicate that the current amount of physical memory is causing a performance bottleneck. This Knowledge Script raises an event if the memory (in KB) swapped-in and swapped-out crosses the threshold you specify.

Note
For Linux and Solaris versions earlier than 2.8, without the swapping scan rate metric, Update Definition in User Variables. monitors the swapping rate.

Resource Object

Memory folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if scan rate exceeds threshold? (y/n)	Set to **y** to raise an event if the scan rate exceeds the threshold. The default is y.
Collect data? (y/n)	Set to **y** to collect data for charts, graphs, and reports. The default is n.
Maximum scan rate (per second)	Type a threshold for the maximum number of pages that should be scanned per second. The default is 0.
Maximum KBytes swapped-in per second threshold	Type a threshold for the maximum amount of memory (in KB) that should be swapped-in per second, for systems without the swapping scan rate metric. The default is 5.
Maximum KBytes swapped-out per second threshold	Type a threshold for the maximum amount of memory (in KB) that should be swapped out per second, for systems without the swapping scan rate metric. The default is 5.
Number of consecutive iterations exceeding threshold before sending an event	Type the number of consecutive times either threshold should be crossed before an event is raised. The default is 2.
Event severity level	Set the event severity level, from 1 through 40, to indicate the importance of the event. The default is 15.

MemUtil

Use this Knowledge Script to monitor physical memory, virtual memory, and paging files. This Knowledge Script raises an event if any usage level crosses the threshold you specify, or if there are any script errors.

Notes

If you install UNIX agent 6.0.2 or 6.5 as a non-root user, this knowledge script displays the following event message:

```
There was trouble parsing output of the command "/opt/netiq/AM/bin/sudo /usr/sbin/
prtconf" for memory size.
```

To resolve, ensure that you include the entries `/usr/sbin/prtconf` and `/usr/sbin/swap` in the `/etc/sudoers` file, manually.

Resource Objects

Physical memory object, virtual memory object, paging files folder.

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if physical memory crosses threshold? (y/n)	Specify whether you want to raise an event if physical memory crosses the thresholds you specify for maximum percentage used or minimum MB free. The default is n. It is normal for UNIX systems to use almost all physical memory.
Raise event if total virtual memory crosses threshold? (y/n)	Specify whether you want to raise and event if virtual memory crosses the thresholds you specify for maximum percentage used or minimum MB free. The default is y.
Raise event if swap space crosses threshold? (y/n)	Specify whether you want to raise an event if the use of the paging file crosses the thresholds you specify for maximum percentage used or minimum MB free. The default is y.
Collect data for physical memory used? (y/n)	Specify whether you want to collect data for charts and reports. If set to y, this script returns the percentage (%) of physical memory in use. The default is n.
Collect data for physical memory free? (y/n)	Specify whether you want to collect data for charts and reports. If set to y, this script returns the amount (in KB) of free physical memory. The default is n.
Collect data for total virtual memory used? (y/n)	Specify whether you want to collect data for charts and reports. If set to y, this script returns the percentage (%) of virtual memory in use. The default is n.
Collect data for total virtual memory free? (y/n)	Specify whether you want to collect data for charts and reports. If set to y, this script returns the amount (in KB) of free virtual memory. The default is n.

Description	How to Set It
Collect data for swap space used? (y/n)	Specify whether you want to collect data for charts and reports. If set to y, this script returns the percentage (%) of the paging file in use. The default is n.
Collect data for swap space free? (y/n)	Specify whether you want to collect data for charts and reports. If set to y, this script returns the amount (in KB) of free paging file space. The default is n.
Threshold -- Maximum physical memory used	Type a threshold for the maximum percentage (%) of physical memory that can be in use before an event is raised. It is normal for UNIX systems to use almost all physical memory. The default is 95%.
Threshold -- Minimum physical memory free	Type a threshold for the minimum amount (in MB) of physical memory that must be free to prevent an event from being raised. The default is 0.
Threshold -- Maximum total virtual memory used	Type a threshold for the maximum percentage (%) of virtual memory that should be in use. The default is 90%.
Threshold -- Minimum total virtual memory free	Type a threshold for the minimum amount (in MB) of virtual memory that should be free. The default is 0.
Threshold -- Maximum swap space used	Type a threshold for the maximum percentage (%) of swap space that should be in use. The default is 70%.
Threshold -- Minimum swap space free	Type a threshold for the minimum amount (in MB) of swap space that should be free. The default is 0.
Event severity -- ...	Set the event severity level, from 1 through 40, to indicate the importance of the event: • ...physical memory. Set the severity level for the event indicating that the maximum physical memory used or minimum physical memory free crosses the threshold. The default is 5. • ...total virtual memory. Set the severity level for the event indicating that the maximum virtual memory used or minimum virtual memory free crosses the threshold. The default is 5. • ...swap space. Set the severity level for the event indicating that the maximum swap space used or minimum swap space free crosses the threshold. The default is 5. • ...when Knowledge Script error occurs. For example, if a Knowledge Script aborts before the job starts or during the job. The default is 10.
HPUX: Include reserved value in calculations? (y/n)	Specify whether you want to include reserved swap space in the calculations. If set to y, calculations will include space reserved system for deactivation and paging processes. This parameter is only available on computers running the HP-UX operating system. The default is y.
HPUX: Include memory pseudo-swap values in calculations? (y/n)	Specify whether you want to include pseudo-swap space in the calculations. Pseudo-swap space might be up to 3/4 of the available system memory. If set to y, calculations will include space in the pseudo swap reservation counters. This parameter is only available on computers running the HP-UX operating system. The default is y.

NetInterfacesCollision

Use this Knowledge Script to monitor network interface collision. The Knowledge Script checks the percentage of network interface collisions in the interval. If the percentage of network interface collisions exceeds the threshold you set, an event is raised.

On AIX, do not use this Knowledge Script to monitor collisions on an Ethernet device. AIX does not provide collision count information for Ethernet devices. If you monitor an Ethernet device on AIX, this Knowledge Script returns a collision count value 0.

This Knowledge Script runs on the Network Interface object. However, it ignores the loopback device.

Note
On Solaris, the UNIX agent must run as root or as a user with root-level authority to retrieve counters associated with the UX Networking performance object. Before running this Knowledge Script, configure the UNIX agent to run as root or as a user that has been given root-level authority using the sudo configuration file.

Resource Objects

Network Interface icon on Solaris, Linux, and HP-UX.

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if network interface collision exceeds the threshold? (y/n)	Set to **y** to raise an event if the percentage of network interface collision exceeds the threshold. The default is y.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is n.
Maximum collision rate (%) threshold	Enter the maximum percentage of network interface collision that should be allowed before raising an event. The default is 80%.
Event severity level	Set the event notification level, from 1 to 40, to indicate the importance of the event. The default severity level is 15.

NetInterfacesConnectivity

Use this Knowledge Script to monitor the physical connection between network interface adapters and the network. If the cable for a network interface card is disconnected from the network, an event is raised.

If the computer where you run this Knowledge Script has only one network interface card and that interface card is unplugged, the event cannot be relayed to the AppManager repository until the network interface card is back in service. Therefore, you should only run this script on computers that have more than one network interface card.

Note
On Solaris, the UNIX agent must run as root or as a user with root-level authority to retrieve counters associated with the UX Networking performance object. Before running this Knowledge Script, configure the UNIX agent to run as root or as a user that has been given root-level authority using the sudo configuration file.

Resource Objects

Network Interface icon on Solaris computers (not supported on Linux, HP-UX, or AIX).

Default Schedule

The default interval for this script is **Asynchronous**. Once you start the Knowledge Script job, its runs continuously on the monitored system and reports events or data as they occur.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if network interface card is disconnected? (y/n)	Set to **y** to raise an event if the cable for a network interface card is unplugged. The default is y.
Event severity when network interface card has lost connectivity	Set the event notification level, from 1 to 40, to indicate the importance of the event. The default severity level is 8.

Example of How this Script Is Used

If you run this Knowledge Script on a computer with multiple network interface cards and at least one of them is available and allows the NetIQ Corporation UNIX agent to communicate with the management server, an event will be raised if any of the network interface cards is disconnected from the network.

Note
This Knowledge Script will not alert you if all network interfaces are disconnected until after network communication is restored. The Knowledge Script job will still raise the event, but the event will be stored in the UNIX agent's local repository until communication with the management server resumes.

NetInterfacesDown

Use this Knowledge Script to monitor the up and down status of network interfaces. This Knowledge Script uses the `ifconfig` command to determine if any network interface card (NIC) on a computer with multiple network interfaces is down. If a network interface is detected down, an event is raised.

If the computer where you run this Knowledge Script has only one network interface card and that interface card is down or unplugged, the event cannot be relayed to the QDB until the card is back in service. Therefore, only run this script on computers with multiple network interface cards.

On Solaris, the UNIX agent must run as root or as a user with root-level authority to retrieve counters associated with the UX Networking performance object. Before running this Knowledge Script, configure the agent to run as root or as a user with root-level authority through the sudo configuration file.

Resource Object

Network Interface icon

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if network interface is down? (y/n)	Set to **y** to raise an event if a network interface is detected down. The default is y.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns a value of 100 if the network interface is up and 0 if the network interface is down. The default is n.
Event severity level	Set the event notification level, from 1 to 40, to indicate the importance of the event. The default severity level is 20.

Example of How this Script Is Used

If you run this Knowledge Script on a computer with multiple network interface cards and at least one of them is available and allows the NetIQ Corporation UNIX agent to communicate with the management server, an event will be raised if any of the network interface cards goes down. In response to the event, you can configure this Knowledge script to run a managed client (MC) action to attempt to bring the NIC back online using the `ifconfig` command and the Action_UXCommand Knowledge Script.

You may also want to use this Knowledge Script in conjunction with other Knowledge Scripts, such as NetInterfacesConnectivity and PingMachine to fine-tune your troubleshooting.

Note
The NetInterfacesDown Knowledge Script will not alert you if all network interfaces are on computer are down until after network communication is restored. The Knowledge Script job will still raise the event, but the event will be stored in the UNIX agent's local repository until communication with the management server resumes.

NetInterfacesErrors

Use this Knowledge Script to monitor the input and output errors for network interfaces. If the number of network interface input errors or output errors exceeds the threshold you set, an event is raised.

This Knowledge Script runs on the Network Interface object. However, the NetInterfacesErrors Knowledge Script ignores the loopback device.

Note
On Solaris, the UNIX agent must run as root or as a user with root-level authority to retrieve counters associated with the UX Networking performance object. Before running this Knowledge Script, configure the UNIX agent to run as root or as a user that has been given root-level authority using the sudo configuration file.

Resource Objects

Network Interface icon.

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if network interface input errors exceed the threshold? (y/n)	Set to **y** to raise an event if the percentage of network interface input errors exceeds the threshold. The default is y.
Collect data on input errors? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the percentage of input errors for the interval. The default is n.
Maximum percentage of input errors (%) threshold	Enter the maximum percentage of network interface input errors that should be allowed before raising an event. The default is 80%.
Event if network interface output errors exceed the threshold? (y/n)	Set to **y** to raise an event if the percentage of network interface output errors exceeds the threshold. The default is y.
Collect data on output errors? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the percentage of output errors for the interval. The default is n.
Maximum percentage of output errors (%) threshold	Enter the maximum percentage of network interface output errors that should be allowed before raising an event. The default is 80%.
Event severity level	Set the event notification level, from 1 to 40, to indicate the importance of the event. The default severity level is 15.

NetInterfacesIO

Use this Knowledge Script to monitor the input and output rate for network interfaces in bytes per second. If the rate of network traffic for input, output, or both exceeds the threshold you set, an event is raised.

This Knowledge Script runs on the Network Interface object. However, the NetInterfacesIO Knowledge Script ignores the loopback device.

Resource Object

Network Interface icon

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data for throughput per second? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the rate of bytes sent and received per second for each interface. The default is n.
Collect data for bytes sent per second? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the rate of bytes sent per second for each interface. The default is n.
Collect data for bytes received per second? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the rate of bytes received per second for each interface. The default is n.
Bytes sent and received per second threshold	Enter a threshold for the maximum number of bytes sent and received per second to monitor the throughput rate for the network interface. The default is 8000000 bytes.
Bytes sent per second threshold	Enter a threshold for the maximum number of bytes sent per second. The default is 8000000 bytes.
Bytes received per second threshold	Enter a threshold for the maximum number of bytes received per second. The default is 8000000 bytes.
Maximum network bandwidth utilization (%) threshold	Enter a threshold for the maximum percent of network bandwidth. The default is 10%.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

PagingHigh

Use this Knowledge Script to monitor UNIX paging activity. If the size in KB paged-in or paged-out per second exceeds the threshold you set, an event is raised.

Resource Object

UNIX computer on Solaris, Linux, and HP-UX (not support on AIX).

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data on page-in KB per second? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the average size in KB paged-in per second. The default is n.
Collect data on page-out KB per second? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the average size in KB paged-out per second. The default is n.
Maximum paged-in KB per second threshold	Enter a threshold for the maximum size in KB for page-in swaps per second. The default is 200.
Maximum paged-out KB per second threshold	Enter a threshold for the maximum size in KB for page-out swaps per second. The default is 200.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

PhysicalDiskBusy

Use this Knowledge Script to monitor physical disk activity and average response time. A disk is considered busy if the percentage of time the disk is in operation is high and the average response time is over the threshold. With this Knowledge Script, you can monitor individual load for individual disks or overall load across all physical disks in a computer.

Note
If both the total disk activity and average response time thresholds are exceeded, the disk is considered overloaded and an event is raised.

Resource Objects

Physical disk folder or individual physical disks.

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the percentage of time the disk is busy and the average response time for requests. The default is n.
Event if disk activity and response time are over the threshold? (y/n)	Set to **y** to raise events when both the disk activity and average response are over their respective thresholds. The default is y.
Average response time maximum threshold (unavailable on AIX)	Enter a threshold for the maximum response time in milliseconds. The default is 200 milliseconds. Do not use this parameter on computers running an AIX operating system.
Maximum physical disk activity (% busy) threshold	Enter a threshold maximum percentage of disk operation before raising an event. The default is 80% busy.
Monitor overall physical disk load? (y/n)	Set to **y** to monitor the overall disk load (for all physical disks on a system). Set to n to monitor individual disks separately.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

PhysicalDiskIO

Use this Knowledge Script to monitor the physical disk I/O activity in kilobytes per second. The Knowledge Script monitors the size of physical disk reads and physical disk writes per second.

On Solaris, Linux, and AIX an event is raised if the size of disk reads per second, the size of disk writes per second, or the overall throughput per second exceeds the threshold you set.

On HP-UX, this Knowledge Script only monitors overall throughput and raises an event if the total size of reads and writes per second is over the threshold.

Resource Object

Physical disk object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is n.
Collect data for reads per second (KB)?	Set to **y** to collect data for charts and reports. If set to y, the script returns the rate of disk read operations in KB per second for each disk. The default is n.
Collect data for writes per second (KB)?	Set to **y** to collect data for charts and reports. If set to y, the script returns the rate of disk write operations in KB per second for each disk. The default is n.
Collect data for throughput per second (KB)?	Set to **y** to collect data for charts and reports. If set to y, the script returns the rate of disk read and write operations in KB per second for each disk. The default is n.
Collect data for reads per second?	Set to **y** to collect data for charts and reports. If set to y, the script returns the number of disk read operations per second for each disk. The default is n.
Collect data for writes per second?	Set to **y** to collect data for charts and reports. If set to y, the script returns the number of disk write operations per second for each disk. The default is n.
Collect data for throughput per second?	Set to **y** to collect data for charts and reports. If set to y, the script returns the number of disk read and write operations per second for each disk. The default is n.
Maximum reads per second (KB) threshold	Enter a threshold for the maximum rate of read operations in KB per second. The default is 50KB per second.
Maximum writes per second (KB) threshold	Enter a threshold for the maximum rate of write operations in KB per second. The default is 50KB per second.
Maximum throughput per second (KB) threshold	Enter a threshold for the maximum rate of read and write operations in KB per second. The default is 100KB per second.
Maximum reads per second threshold	Enter a threshold for the maximum number of read operations per second. The default is 50 operations per second.
Maximum writes per second threshold	Enter a threshold for the maximum number of write operations per second. The default is 50 operations per second.

Description	How to Set It
Maximum throughput per second threshold	Enter a threshold for the maximum number of read and write operations per second. The default is 100 operations per second.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

PingMachine

Use this Knowledge Script to check the availability of any computers or other devices that reply to ICMP Echo requests. (The ICMP Echo request is commonly used by the `ping` command on UNIX and Windows computers.) With this Knowledge Script, you can check the up/down status of your managed UNIX computers, Windows computers, and other equipment, such as TCP/IP-based printers.

You can specify computers to ping in two ways: by providing comma-separated lists or by naming files containing comma-separated lists. If a computer does not respond to a ping within the response time threshold, the script raises an event.

There are separate lists for UNIX and Windows computers. This separation allows the script to push raised events to computers listed in your TreeView: to do this, the script needs to know whether an event is destined for a UNIX or Windows computer. When an event is pushed to a computer listed in your TreeView, its icon blinks.

This script can raise an event for a computer that is not listed in your TreeView. When this happens, a server group named AppManager Proxy Events is automatically created in the Master TreeView. From this group, you can view, acknowledge, close, and delete all events on the computer. To discover resources and run monitoring jobs on the computer, you must delete the computer from the AppManager Proxy Events server group, then manually add the computer to the TreeView. If necessary, stop any proxy jobs that are monitoring the remote computer so you can add it to the TreeView.

Resource Object

UNIX computer icon

Default Schedule

The default interval for this script is **Every two hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
List of UNIX machines to check (by hostname or IP address)	Enter a list of UNIX computer names, separated by commas, that you want to test communication with. For example: `localhost,www.netiq.com`
List of Windows machines to check (by hostname or IP address)	Enter a list of Windows computer names, separated by commas, that you want to test communication with. For example: `us.sandiego01.com,us.portland01.com`

Optional file listing UNIX hosts to ping	Type the full path to the file containing a list of the UNIX computers you want to check. The file should contain the hostname or IP address for each computer in one or more lines. Each line can have multiple computer names, separated by commas. For example:
	`NYC01,NYC02`
	`SALES01,10.15.221.5, SFO01`
	`LABMACH, QATEST`

Description	How to Set It

Optional file listing Windows hosts to ping	Type the full path to the file containing a list of the Windows computers you want to check. The file should contain the hostname or IP address for each computer in one or more lines. Each line can have multiple computer names, separated by commas. For example:
	`NYC01,NYC02`
	`SALES01,10.15.221.5, SFO01`
	`LABMACH, QATEST`

Collect data for response time? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the time it took the server to respond to the `ping` command. The default is n.
Collect data for machine up/down? (y/n)?	Set to **y** to collect data for charts and reports. If set to y, the script returns: • 100 -- Computer tested sent a reply indicating a successful connection, or • 0 -- There was no reply. The default is n.
Event if response time exceeds the threshold? (y/n)	Set to **y** to raise an event if the response time for the response from the computer whose connection you are testing exceeds the threshold you set. By default, events are raised.
Event if machines is not responding? (y/n)	Set to **y** to raise an event if the computer whose connection you are testing fails to respond to the Ping test. By default, events are raised.
Maximum response time (ms) threshold	Enter a threshold for the maximum response time in milliseconds for the reply to take. The default is 500 milliseconds.
Event severity when...	Set the event severity level, from 1 to 40, to indicate the importance of each event. By default, the severity levels are: • **... response time is exceeded**. The default severity is 15 • **... the machine is unreachable**. The default severity is 5
Number of times to ping target machine per iteration	Enter the number of times that you want to ping the target computer for each iteration. The default is 1.

PortHealth

Use this Knowledge Script to check whether system ports are working properly. This Knowledge Script raises an event if a port is not operating properly.

There are separate lists for UNIX and Windows computers. This separation allows the script to push raised events to computers listed in your TreeView: to do this, the script needs to know whether an event is destined for a UNIX or Windows computer. When an event is pushed to a computer listed in your TreeView, its icon blinks.

This script can raise an event for a computer that is not listed in your TreeView.

Note
This Knowledge Script raises an event if a port specified for monitoring cannot be reached from the computer where you dropped the Knowledge Script. If you entered the computer name correctly as a Windows or UNIX computer, and it is displayed in the TreeView pane, the computer's icon blinks, indicating that it did not respond. If the computer is not displayed in the TreeView pane, the icon for the computer where you dropped the Knowledge Script blinks.

Resource Object

UNIX computer icon

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if port cannot be reached? (y/n)	Set to **y** to raise an event if a specified port is not operating properly. The default is y.
Collect data for port status? (y/n)	Set to **y** to collect data for graphs and reports. If enabled, returns: • 100 -- the port is operating properly, or • 0 -- the port is not operating. The default is n.
Windows network addresses in format hostIP:port_number (separated by commas, no spaces)	Type one or more Windows network addresses using the format *host_IP*:*port_number*. Separate multiple addresses by commas and no spaces. The *host_IP* can be a hostname or an IP address. For example: `www.storm.com:8008,21.1.10.1:30`. The default is `www.netiq.com:80`.
UNIX network addresses in format hostIP:port_number (separated by commas, no spaces)	Type one or more UNIX network addresses using the format *host_IP*:*port_number*. Separate multiple addresses by commas and no spaces. The *host_IP* can be a hostname or an IP address. For example: `www.storm.com:8008,21.1.10.1:30`.
Event severity when port cannot be reached	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

PrinterQueue

Use this Knowledge Script to monitor the health of printers. This Knowledge Script checks the number of jobs in printer queue and the size of the printer queue in KB. If either the number of jobs waiting or the queue size exceeds the threshold you set, an event is raised.

Note
General printer status information, such as when the printer is taken off-line or is low on toner, cannot be detected by this Knowledge Script.

Resource Objects

UNIX Printer objects

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if printer queue exceeds the threshold? (y/n)	Set to **y** to raise an event if the number of jobs in the printer queue exceeds the threshold. The default is y.
Event if printer queue size (KB) exceeds the threshold? (y/n)	Set to **y** to raise an event if the size of the printer queue, in KB, exceeds the threshold. The default is y.
Collect printer queue length data?	Set to **y** to collect data for charts and reports. The default is n. If you collect data, the Knowledge Script reports the number of print jobs in the queue at each interval.
Collect printer queue size data?	Set to **y** to collect data for charts and reports. The default is n. If you collect data, the Knowledge Script reports the size in KB of the printer queue at each interval.
Maximum number of jobs in the printer queue threshold	Enter a threshold for the maximum number of print jobs waiting in the queue. The default is 100 jobs.
Maximum printer queue size (KB) threshold	Enter a threshold for the maximum size of the printer queue in KB. The default is 4000 KB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

PrivilegedProcs

Use this Knowledge Script to monitor the number of system processes with an effective user id (`euid`) of `root`. You can specify one or more processes to exclude from the list, if needed. If the number of processes running under `root` is over the threshold you set, an event is raised.

Resource Object

UNIX CPU folder

Default Schedule

The default interval for this script is **Every hour.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if over the threshold? (y/n)	Set to **y** to raise an event if the number of processes running under the root user exceeds the threshold. The default is y.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is n. If you collect data, the Knowledge Script reports the number of processes owned by the root user at each interval.
Maximum number of processes owned by root threshold	Enter a threshold for the maximum number of processes owned by the root user. The default is 30 processes.
Processes to exclude separated by commas	Enter the processes you want to exclude from the list of processes owned by root. Use a comma with no spaces to separate process names.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

ProcessDown

Use this Knowledge Script to determine whether specified processes are currently running. An event is raised if a specified process is not running or if the minimum number of processes are not running.

Resource Object

UNIX CPU folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise an event if the process is not running? (y/n)	Set to **y** to raise events. The default is y.
Collect data for processes not running? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns data for each named process. A value of 100 is returned if the process is running; a value of 0 is returned if the process is not running. The default is n.
Processes to monitor (comma-separated)	Enter one or more process names, separated by commas and no spaces. For example: `grep,batch`
Minimum number of each process required (comma-separated)	Enter the minimum number of instances that have to go down before you want AppManager to raise an event. If you are monitoring more than one process, list the numbers for each process separated by commas and no spaces. The default is 1. For example, if you do not want to raise an event every time the grep and batch processes goes down, but you do want to raise an event after 10 instances of the process go down, enter: `10,10`
Event severity when process is down	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

Processes

Use this Knowledge Script to monitor the number of processes. If the total number of processes detected exceeds the threshold you set, an event is raised.

Resource Object

UNIX CPU folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if over the threshold? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the total number of processes running on the system. The default is n.
Maximum number of processes threshold	Enter a threshold for the maximum number of processes. The default is 100 processes.
Monitor process count for just specified user	Specify a user account if you want to monitor the number of processes started by that user.
Processes to exclude separated by commas	Enter the names of any processes you want to exclude from the list of processes found. Use a comma with no spaces to separate process names.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

ProcessUp

Use this Knowledge Script to check whether a specified process is running. If the specified process is running, an event is raised. You also have the option to automatically terminate the process.

Resource Object

UNIX CPU folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise an event if the process is running? (y/n)	Set to **y** to raise events. The default is y.
Collect data for processes running? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns a value of 100 when the number of running processes exceeds the threshold, or a value of 0 when the number of running process does not exceed the threshold. The default is n.
Processes for which to look (comma-separated)	Enter one or more process names, separated by commas and no spaces. For example: `grep,batch`
Maximum number of each process required (comma-separated)	Enter the number of instances required to generate an event for each process, separated by commas and no spaces. AppManager will report an event when the number of instances is running for each process. The default is 0,0. For example: `3,4`
Kill the running process? (y/n)	Set to **y** to kill the specified processes if they are detected running. The default is n.
Event severity level...	Set the event severity level, from 1 to 40, to indicate the importance of each event. • **... for process running**. Set a value to indicate a specified process was detected up. The default is 10. • **... for failed to kill process**. Set a value to indicate a specified process was detected up but the attempt to kill the process failed. The default is 10.

RemoteProcessDown

Use this Knowledge Script to monitor processes on a remote UNIX computer where you have not installed the UNIX agent. This Knowledge Script runs on a proxy UNIX agent and monitors processes on a remote UNIX computer.

When you drag this Knowledge Script to a UNIX computer in the TreeView, the Knowledge Script runs on that computer and tries to communicate with a specified list of remote UNIX computers. This Knowledge Script raises an event if any of the named processes are down or any of the computers you specify cannot be reached from the computer where this Knowledge Script is running.

If a monitored process is found to be down, this Knowledge Script can restart it using a script or command you supply. Be sure to read the help for the **Scripts or commands to restart processes** parameter, below, before proceeding.

Resource Object

UNIX computer icon (not supported on HP-UX Itanium).

Default Schedule

The default interval for this script is **Every 10 minutes**.

If the script used to restart any process found to be down takes a considerable amount of time, events generated by the job will be generated more than 10 minutes apart (by default).

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Raise event if process is down?	Select **yes** to raise an event if the monitored process is found to be down. By default, events are enabled.
Event severity when process is down	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Raise event if process is running?	Select **yes** to raise an event if the monitored process is found to be running. By default, events are not raised.
Event severity when process is running	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Remote Host Connection Configure access to the remote managed computers by specifying their root password. All of the remote computers must use the same root password. This Knowledge Script can use SSH with root password authentication or Telnet to communicate with the remote managed computer.	
Password for root user account	If you want to use Secure Shell (SSH) for the connection to the remote computers, make sure SSH with root authentication is enabled on the remote UNIX computers where you want to install the UNIX agent. For this parameter, you must specify the password for the root user to securely access the remote UNIX computers. This Knowledge Script does not support SSH root authentication with an RSA key.

Description	How to Set It

Connection Transport	Select either SSH/SFTP or Telnet/FTP. The default is Telnet/FTP,
	This Knowledge Script can use SSH with root password authentication or Telnet to communicate with the remote managed computer.
	If you select the Telnet/FTP option the Telnet prompt on the remote computer must end with a space or one of the following characters:
	`%`
	`>`
	`#`
	`$`
	This example shows a supported Telnet prompt:
	`user@hostname>`
	This example shows an unsupported Telnet prompt:
	`<user@hostname:/tmp - 2005-Mar-09>`
	`->`
	In the examples above, the last character in the first line of the 2-line prompt is a line feed character, which is not supported.

Telnet non-root user account	If you selected Telnet to connect to the remote UNIX computers, specify a non-root user account to use for the connection. When connecting to a remote UNIX computer using Telnet and FTP, this Knowledge Script switches from the non-root user to the root user.
Telnet non-root user account password	If you selected Telnet as the connection transport medium, specify the password for the non-root user account to connect to the remote UNIX computers.
Proxy Monitoring Configuration	
Full path to configuration file for remote monitoring	Supply a full directory path to an XML file to use for monitoring instructions. The configuration file should specify which processes to monitor on the remote UNIX computer and how to restart them. See "Remote Process Monitoring Using a Configuration File" on page 3902 for more information about the configuration file. The default is `/tmp/config.xml`.
Monitoring without Configuration File	
Hostnames or IP addresses where processes are to be monitored (comma-separated)	Enter a list of hostnames or IP addresses of the UNIX computers where processes are to be monitored. Separate multiple hostnames with commas (,) and no spaces. Supply IP addresses in dotted notation, such as 23.45.678.9. Separate multiple IP addresses with commas and no spaces.
Names of processes to monitor (comma-separated)	Supply the names of the UNIX application processes to monitor. Separate multiple process names with commas and no spaces. You can also enter a Perl regular expression here if you want to exclude and include processes on various platforms through the use of one argument. See "Running this Knowledge Script" on page 3901 for more information.

Description	How to Set It
Scripts or commands to restart processes (comma-separated)	Supply one of the following: • a list of full directory paths to script files to use to restart any processes that are found to be down, or • a list of commands to use to restart these processes. Use this parameter only when you restart the process when it is down. Specify a list of restart commands or shell scripts that contain the restart commands. Do not execute restart commands in the foreground. When executing a restart command in the foreground, this Knowledge Script cannot run at its next scheduled interval until after all of the restart commands have completed. When specifying: • A list of commands to run on the remote computer, run each command in the background by appending an ampersand (&) and separate each command with a comma. If this Knowledge Script is configured to use Telnet/FTP, you can restart a process in the background by appending an ampersand (&) to each command. If this Knowledge Script is configured to use SSH/SFTP, you should use a shell script on the remote computer to restart the processes in the background and ensure that `stdout` and `stderr` are redirected to a log file. When configured to use SSH/SFTP, this Knowledge Script always executes a command to restart a process in the foreground. • A shell script on the remote computer that restarts the processes you want, in the shell script, append an ampersand (&) to each restart command--and ensure that `stdout` and `stderr` are redirected to a log file--to restart a process in the background.
Restart process if down? (y/n for each process, comma-separated)	Provide a list specifying "y" or "n" for each process in the list of processes to monitor. Specify y for a process if you want this Knowledge Script to restart it on the remote computer if it is found to be down. The commands or scripts you specified for the previous parameter will be used. Separate each entry in the list with a comma. Do not use spaces.

Running this Knowledge Script

This Knowledge Script requires the proxy UNIX agent to run as the root user account.

It can use either the Secure Shell (SSH) program with root password authentication or Telnet to make a secure connection to the remote UNIX computer(s). By default, Telnet is used, but you can select SSH/SFTP from the **Connection Transport** list to use Secure Shell instead. If you choose to use Telnet, you must supply a non-root user account name and password.

Notes

Proxy monitoring with this Knowledge Script is possible only if the SSH program is installed on the target computer, or if the Telnet protocol is enabled on it.

A version of this Knowledge Script that runs on a Windows proxy computer to monitor remote UNIX computers is also available. See the NT_UnixRemoteProcessDown Knowledge Script.

You can use this Knowledge Script to monitor the up and down status of the UNIX agent. To do this, specify `nqmagt` in the list of processes you want to monitor. If the `nqmagt` process is detected down, you can specify a restart command, `/etc/init.d/nqmdaemon start`, to restart the agent.

You can specify the process names to be monitored as a parameter, or you can provide a configuration file in XML format to specify processes to monitor and what steps to take to restart them if they're down. See "Remote Process Monitoring Using a Configuration File" on page 3902 for more information about the configuration file.

You can also supply a Perl regular expression for the **Names of processes to monitor (comma-separated)** parameter if you want to check for a specific string. For example, you can exclude and include processes on various platforms through the use of one argument. Let's assume that a process is running out of the `/usr`, the `/opt`, or the `/var` directory, but you're not sure where. Or perhaps a process may run out of different locations on different platforms. You might enter `(/usr|/opt)/[processname]` for the **Names of processes to monitor** parameter. The Knowledge Script would monitor the process that is running in `/usr` OR in `/opt` but NOT in `/var`. The topic titled "Creating Filters with Regular Expressions" on page 3842 contains more information about regular expressions.

Remote Process Monitoring Using a Configuration File

The RemoteProcessDown Knowledge Script includes an option to use a configuration file in XML format to supply monitoring instructions to the agent. In such a file, you can supply a list of processes to monitor on a given remote UNIX computer, specify how to restart these processes, and indicate whether to restart these processes.

By default, the Knowledge Script looks for the following configuration file:

```
/tmp/config.xml
```

However, you can supply a different file as the value for the **Full path to configuration file for remote monitoring** parameter.

Following is an example of a valid XML configuration file that instructs the UNIX agent which processes to monitor and what to do if they're found not running:

```
<?xml version="1.0" encoding="utf-8" ?>
<SERVERS>
  <SERVER name="uws3">
    <PROCESS name="nqmagt" startupscript="/etc/init.d/nqmdaemon start" restart="y"/>
<PROCESS name="xntpd"  startupscript="/etc/init.d/xntpd start" restart="n"/>
</SERVER>
  <SERVER name="uws19">
     <PROCESS name="inetd"  startupscript="/etc/init.d/inetsvc start" restart="n"/>
<PROCESS name="init"  startupscript="/etc/init.d/init start" restart="n"/>
</SERVER>
       </SERVERS>
```

Report_CPULoad

Use this Knowledge Script to generate a detailed report about CPU usage. Using this report, you can aggregate the data by time period (minute, hour, or day) and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the CpuLoaded Knowledge Script.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*.

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *UNIX_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all the data streams on a single page The default is By computer.
Select time range	Click the **Browse [...]** button to start the time wizard. Use the time wizard to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending at the current time.
Select peak weekday(s)	Click the **Browse [...]** button to start the day wizard. Use the day wizard to select the days of the week to include in your report. The default is seven days: Sunday through Saturday.
Aggregation by	Specify how you want to aggregate the data in your report. You can specify Minute, Hour, or Day. The default is Hour.
Aggregation interval	Specify the intervals you want to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card? (yes/no)	Specify whether you want to include a table in the report that lists parameter settings for the report script. By default, the table is included.
Include table/chart/both?	Select whether you want to include a table, a chart, or both of data stream values in the report. By default, the table is included.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box and select the graphic properties for the charts in your report. The default is Bar.
Select output folder	Click the **Browse [...]** button to open the Publishing Options dialog box and select the parameters for your report's output folder. The default folder prefix is UNIX_CPULoad.
Add job ID to output folder name? (yes/no)	Specify whether you want to add the job ID to the report's output folder name. The default is no. Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box and select the properties as desired. The default title for your report is UNIX CPU Load.
Add time stamp to title? (yes/no)	Specify whether you want to append a time stamp to the title of your report, making each title unique. The time stamp includes the date and time the report was generated. The default is no. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success? (yes/no)	Specify whether you want to raise an event if the report is successfully generated. By default, events are enabled.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of the event for: • ...**report success**. The default is 35. • ...**report with no data**. The default is 25. • ...**report failure.** The default is 5.

Report_DiskUsageSummary

Use this Knowledge Script to generate a summary report about the percentage of disk space used and the amount of free space (in MB). Using this report, you can develop a statistical summary of the data you select, for example, the average value of data points over the time period you define for the report.

This report uses data collected by the FileSystemSpace Knowledge Script.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*.

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse [...]** button to start the time wizard. Use the time wizard to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending at the current time.
Select peak weekday(s)	Click the **Browse [...]** button to start the day wizard. Use the day wizard to select the days of the week to include in your report. The default is seven days: Sunday through Saturday.
Select the style	Select the style for the first page of your report: • **By computer** displays one value for each computer you selected. • **By legend** displays one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** displays one value for each unique legend from each computer. The default is By computer and legend.
Data settings	Use the following parameters to select the data settings for your report.

Description	How to Set It
Statistics to show	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the time range of the report. • **Minimum**. The minimum value of data points for the time range of the report. • **Maximum**. The maximum value of data points for the time range of the report. • **Min/Avg/Max**. The minimum, average, and maximum values of data points for the time range of the report. • **Range**. The range of values in the data stream (maximum - minimum = range). • **StandardDeviation**. The measure of how widely values are dispersed from the mean. • **Sum**. The total value of data points for the time range of the report. • **Close**. The last value for the time range of the report. • **Change**. The difference between the first and last values for the time range of the report (close - open = change). • **Count**. The number of data points for the time range of the report. The default is Average.
Select sorting or display options	Specify whether you want to sort data in your report or how you want to display the data: • **No sort**. Data is not sorted. • **Sort**. Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right). • **Top %**. Chart only the top N % of selected data (sorted by default). • **Top N**. Chart only the top N of selected data (sorted by default). • **Bottom %**. Chart only the bottom N % of data (sorted by default). • **Bottom N**. Chart only the bottom N of selected data (sorted by default). The default is No sort.
Percentage (%) or count for top or bottom of chart	Type a number for either the percent or count defined in **Select sorting or display options** (for example, Top 10%, or Top 10). The default is 25.
Truncate top or bottom? (yes/no)	Specify whether you wan to truncate the top or bottom data in your report. If set to yes, the data table displays only the top or bottom N or % (for example, only the top 10%). If set to no, the table displays all data. The default is no.
Show totals on the table? (yes/no)	Specify whether you want to display additional calculations for each column of numbers in a table. If set to yes, the following values are listed at the end of the table: • **Report Average**. An average of all values in a column. • **Report Minimum**. The minimum value in a column. • **Report Maximum**. The maximum value in a column. • **Report Total**: The total of all values in a column. The default is no.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card? (yes/no)	Specify whether you want to include a table in the report that lists parameter settings for the report script. By default, the table is included.
Include table/chart/both?	Select whether you want to include a table, a chart, or both of data stream values in the report. By default, the table is included.

Description	How to Set It
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box and select the graphic properties for the charts in your report. The default is Bar.
Select output folder	Click the **Browse [...]** button to open the Publishing Options dialog box and select the parameters for your report's output folder. The default folder prefix is UNIX_LogicalDiskUsageSummary.
Add job ID to output folder name? (yes/no)	Specify whether you want to add the job ID to the report's output folder name. The default is no. Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box and select the properties as desired. The default title for your report is UNIX Logical Disk Usage Summary.
Add time stamp to title? (yes/no)	Specify whether you want to append a time stamp to the title of your report, making each title unique. The time stamp is made up of the date and time the report was generated. The default is no. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success? (yes/no)	Specify whether you want to raise an event if the report is successfully generated. By default, events are enabled.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of the event for: • ...**report success**. The default is 35. • ...**report with no data**. The default is 25. • ...**report failure**. The default is 5.

Report_MemoryUtilization

Use this Knowledge Script to generate a report about the use of physical and virtual memory, and paging files. Using this report, you can aggregate data by time period (minute, hour, or day) and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the MemUtil Knowledge Script.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*.

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *UNIX_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all data streams on a single page The default is By computer.
Select time range	Click the **Browse [...]** button to start the time wizard. Use the time wizard to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending at the current time.
Select peak weekday(s)	Click the **Browse [...]** button to start the day wizard. Use the day wizard to select the days of the week to include in your report. The default is seven days: Sunday through Saturday.
Aggregation by	Specify how you want to aggregate the data in your report. You can specify Minute, Hour, or Day. The default is Hour.
Aggregation interval	Specify the intervals you want to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card? (yes/no)	Specify whether you want to include a table in the report that lists parameter settings for the report script. By default, the table is included.
Include table/chart/both?	Select whether you want to include a table, a chart, or both of data stream values in the report. By default, the table is included.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box and select the graphic properties for the charts in your report. The default is Bar.
Select output folder	Click the **Browse [...]** button to open the Publishing Options dialog box and select the parameters for your report's output folder. The default folder prefix is UNIX_MemoryUtilization.
Add job ID to output folder name? (yes/no)	Specify whether you want to add the job ID to the report's output folder name. The default is no. Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box and select the properties as desired. The default is UNIX Memory Utilization.
Add time stamp to title? (yes/no)	Specify whether you want to append a time stamp to the title of your report, making each title unique. The time stamp is made up of the date and time the report was generated. The default is no. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success? (yes/no)	Specify whether you want to raise an event if the report is successfully generated. By default, events are enabled.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of the event for: • ...report success. The default is 35. • ...**report with no data**. The default is 25. • ...**report failure**. The default is 5.

Report_NetInterfacesIO

Use this Knowledge Script to generate a report about the use of bandwidth on network interface cards. Using this report, you can aggregate data by time period (minute, hour, or day) and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the NetInterfacesIO Knowledge Script.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*.

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select the style	Select the style for the first page of your report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the *UNIX_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** provides all the data streams on a single page The default is By computer.
Select time range	Click the **Browse [...]** button to start the time wizard. Use the time wizard to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending at the current time.
Select peak weekday(s)	Click the **Browse [...]** button to start the day wizard. Use the day wizard to select the days of the week to include in your report. The default is seven days: Sunday through Saturday.
Aggregation by	Specify how you want to aggregate the data in your report. You can specify Minute, Hour, or Day. The default is Hour.
Aggregation interval	Specify the intervals you want to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in your report: • **Average**. The average value of data points for the aggregation interval (for example, the average value for 1 Hour). • **Minimum**. The minimum value of data points for the aggregation interval. • **Maximum**. The maximum value of data points for the aggregation interval. • **Count**. The number of data points for the aggregation interval. • **Sum**. The total value of data points for the aggregation interval. • **3Sigma**. The average + (3 * standard deviation) and average - (3 * standard deviation). • **Std**. The standard deviation. The measure of how widely values are dispersed from the mean. • **Box**. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval. • **Open**. The first value for the aggregation interval. • **Close**. The last value for the aggregation interval. The default is Average.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card? (yes/no)	Specify whether you want to include a table in the report that lists parameter settings for the report script. By default, the table is included.
Include table/chart/both?	Select whether you want to include a table, a chart, or both of data stream values in the report. By default, the table is included.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box and select the graphic properties for the charts in your report. The default is Bar.
Select output folder	Click the **Browse [...]** button to open the Publishing Options dialog box and select the parameters for your report's output folder. The default folder prefix is UNIX_NetInterfacesTraffic.
Add job ID to output folder name? (yes/no)	Specify whether you want to add the job ID to the report's output folder name. The default is no. Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box and select the properties as desired. The default title for your report is Network Interface Card Traffic.
Add time stamp to title? (yes/no)	Specify whether you want to append a time stamp to the title of your report, making each title unique. The time stamp is made up of the date and time the report was generated. The default is no. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success? (yes/no)	Specify whether you want to raise an event if the report is successfully generated. By default, events are enabled.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of the event for: • ...**report success**. The default is 35. • ...**report with no data**. The default is 25. • ...**report failure**. The default is 5.

Report_SystemUpTime

Use this UNIX Report Script to generate a report detailing the uptime and downtime of monitored computers. Uptime and downtime are illustrated in hours and minutes, as well as the percentage of the monitoring interval during which a computer is running or not. For example, if during a 24-hour monitoring interval, the computer is running for 18 hours and not running for 6 hours, the uptime and downtimes are represented as:

- Uptime: 18 hours 0 minutes
- Downtime: 6 hours 0 minutes
- Uptime: 75%
- Downtime: 25%

This report uses data collected by the SystemUpTime Knowledge Scripts. In order to have accurate data for this report, these Knowledge Scripts should be scheduled to run every 5 minutes.

Uptime and downtime are calculated during scheduled maintenance. Ad hoc maintenance is considered as downtime, and is included in all calculations.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*.

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select the style	Select the style for the first page of the report: • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page The default is By computer and data stream.
Select time range	Click the **Browse [...]** button to start the time wizard. Use the time wizard to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending at the current time.
Select peak weekday(s)	Click the **Browse [...]** button to start the day wizard. Use the day wizard to select the days of the week to include in your report. The default is seven days: Sunday through Saturday.

Description	How to Set It
Aggregation interval	Select the time period by which the data in your report is aggregated: • Hourly • Daily • Weekly The default is Hourly.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card?	Set to **y** to include a card in the report that lists parameter settings for the report script. The default is to include the card.
Include table/chart/both?	Select whether you want to include a table, a chart, or both of data stream values in the report. By default, the table is included.
Select chart style	Click the **Browse [...]** button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report. The default is a line chart.
Select output folder	Click the **Browse [...]** button to set parameters for the output folder. The default output folder prefix is SystemUpTime.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box. Set the properties parameters as desired. The default report title is SystemUp Time.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. The default is n. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success?	Set to **y** to raise an event when the report is successfully generated. The default is to enable the event.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Report_TopMemoryProcs

Use this Knowledge Script to generate a report about the total memory used by all processes and which processes consume the most memory resources.

This report uses data collected by the TopMemoryProcs Knowledge Script.

Resource Objects

Report Agent > AM Repositories > *AppManager repository*.

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report. **Note** For this report, select only one View, and up to 15 computers or server groups. The data wizard allows you to select more, but if you do, the Finish button is disabled. This mechanism prevents you from selecting too much data for the report.
Select time range	Click the **Browse [...]** button to start the time wizard. Use the time wizard to set a specific or sliding time range for data included in your report. The default is Sliding Time: 1 Day ending at the current time.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card? (yes/no)	Specify whether you want to include a table in the report that lists parameter settings for the report script. By default, the table is included.
Select output folder	Click the **Browse [...]** button to open the Publishing Options dialog box and select the parameters for your report's output folder. The default prefix for the folder name is UNIX_TopMemoryProcs.
Add job ID to output folder name? (yes/no)	Specify whether you want to add the job ID to the report's output folder name. The default is no. Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click the **Browse [...]** button to open the Report Properties dialog box and select the properties as desired. The default title is UNIX Top Memory Utilization by Process.
Event Notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.

Description	How to Set It
Event for report success? (yes/no)	Specify whether you want to raise an event if the report is successfully generated. By default, events are enabled.
Severity for report...	Set the event severity level, from 1 to 40, to indicate the importance of the event for: • ...success. The default is 35. • ...with no data. The default is 25. • ...failure. The default is 5.

RunAwayProcs

Use this Knowledge Script to detect runaway processes on the specified computer by repeatedly sampling CPU usage for processes. If a process exceeds the CPU threshold in the number of consecutive samples taken (one at each interval), an event is raised.

For example, if this Knowledge Script detects that a process has exceeded the CPU threshold for five consecutive monitoring periods, it may indicate that the process is trapped in an infinite loop or has encountered other problems. In addition to generating an event to notify you of the problem, you can optionally kill any detected runaway processes. The detail message shows the list of processes being sampled.

Resource Object

UNIX computer icon

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. The default is n.
Maximum CPU usage (%) for runaway processes	Enter a threshold for the maximum percentage of CPU any process should be using when sampled. This percentage is used to determine which processes are runaway processes. The default is 90%.
Number of consecutive samples to take	Enter the number of consecutive samples you want taken before raising an event. The default is 3 samples.
Number of runaway processes to show (0 = all)	Specify the number of processes you want displayed in detail event or data message. Enter 0 if you want all processes displayed. The default is 0 for all processes.
Ignore these comma-separated processes	Enter the names of any processes (separated by commas and no spaces) you want to exclude from sampling.
Never kill these comma-separated processes	Enter the names of any processes (separated by commas and no spaces) that should never be killed. The default processes are `sched`, `init`, `pageout`, `fsflush`, `inetd`, `yp`, and `rpc`.
Kill runaway process when detected? (y/n)	Set to **y** to kill any runaway processes found automatically (with the exception of the processes you have specified should never be killed). The default is n.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of each event: • **... runaway process detected**. The default is 5. • **... killed runaway process**. The default is 10. • **... failed to kill runaway process**. The default is 10.

RunCommand

Use this Knowledge Script to run a non-interactive UNIX command. For example, you can use this Knowledge Script to run a batch command that appends a log file or kills a process.

This Knowledge Script raises an event if the results of the command produce output. You can configure this Knowledge Script to not raise an event if the results of the command do not produce any output.

Resource Object

UNIX computer icon

Default Schedule

By default, this script is only run once per computer.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event displaying text sent to STDOUT?	Specify whether you want to raise an event containing the STDOUT of the executed command. The default is y.
Include STDERR in event text?	Specify whether you want to include the STDERR of the command along with the STDOUT in the event text. The default is y.
Raise event if output is empty?	Specify whether you want to raise an event if the results of the command do not produce any output. The default is y.
UNIX command with possible arguments	Type the command to run. Do not enter a command that requires user input. The command you enter should include all necessary arguments and handle any input and output redirection or file management required. Separate multiple processes with semicolons (;) and no spaces.
Event severity level for STDOUT/STDERR event	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 22.

SwapLow

Use this Knowledge Script to monitor the swap area (files and/or devices) available. You can monitor the overall percentage of space available across all swap areas, or monitor individual swap areas separately. If the percentage of available swap area is below the threshold you set, an event is raised.

Resource Objects

Swap folder or individual swap area objects.

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if under the threshold? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. The default is n.
Minimum swap space available (%) threshold	Enter a threshold for the minimum percentage of swap space that should be available. The default is 3%.
Monitor overall swap space availability? (y/n)	Set to **y** to monitor all swap areas on a system. Set to n to monitor individual swap areas separately (multiple data streams may be created). The default is n.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event**.** The default is 20.

Syslog

Use this Knowledge Script to monitor the `syslog` file asynchronously for specific messages or search strings. You can enter the search strings to look for using regular expressions and modifiers to define an Include filter and an Exclude filter or you can enter your search criteria in a separate filter file and use this Knowledge Script to specify the location of that file.

You can use just the Include filter, just the Exclude filter, or both. If you use both filters, messages that contain any included search strings and do not contain any of the excluded search strings are returned.

To specify the include and exclude patterns, you need to be familiar with Perl regular expressions. Some information is available in the topic "Creating Filters with Regular Expressions" on page 3842.

Notes

On all platforms, the UNIX agent must run as root or as a user with root-level authority to configure and retrieve information from the syslog file. Before running this Knowledge Script, configure the UNIX agent to run as root or as a user that has been given root-level authority using the sudo configuration file. SuSE10 no longer supports syslogd because it has introduced an upgraded syslog named syslogd-ng. However, if you need monitoring support for syslogd, you need to install and configure the earlier, bsd-based syslogd.

The SysLog Knowledge Script creates a synchronized duplicate of the syslog file in $AM_HOME/log/, and uses the duplicate rather than the UNIX syslog file. If this is a security concern, either take measures to protect this file or do not run the script.

Resource Object

UNIX computer icon

Default Schedule

The default interval for this script is **Asynchronous**. Once you start the Knowledge Script job, its runs continuously on the monitored system and reports events or data as they occur.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, the script returns the number of messages matching the search criteria. The default is n.
Event message to display (clearing this setting will display the matched line)	Type the event message you want to display when messages matching the search criteria are found. If you leave this field blank, the entry in the syslog file that matched your search criteria is displayed as the event message. If you specify a custom event message, you can still view the matching entry from the syslog file by displaying the Properties for the child event and clicking the **Message** tab. The default event message is: Syslog match found

Description	How to Set It
Regular expression specifying the include filter	Type a regular expression, in Perl, to identify the pattern you want to look for in the text file being monitored. Strings matching the include filter pattern are returned. The default expression matches all strings. For information about writing Perl regular expressions, see Creating Filters with Regular Expressions.
Modifier for the regular expression include filter	Optional modifiers can be used to change the behavior of the regular expression. For example, specifying "i" for this parameter makes the include filter case-insensitive. To use the case-insensitive modifier, you would type: `i`
Regular expression specifying the exclude filter	Type a regular expression, in Perl, to identify the pattern you want to exclude from matching in the text file being monitored. Strings matching the include filter pattern are returned. For information about writing Perl regular expressions, see Creating Filters with Regular Expressions.
Modifier for the regular expression exclude filter	Optional modifiers can be used to change the behavior of the regular expression. For example, specifying "i" for this parameter makes the exclude filter case-insensitive.
Optional file containing additional filters	Enter the full path to a file containing any additional filter items you want to match. You can also use this parameter if you only want to specify matching expressions in an external file.
Ignore syslog timestamp?	Set to **y** if you want to disregard the time when the event was raised. The default is n.
Event severity level	Set the event notification level, from 1 to 40, to indicate the importance of the event. By default, the severity level is 8.

Example of How this Script Is Used

This Knowledge Script allows you to specify include and exclude expressions as Knowledge Script properties or maintain your search criteria independent of the Knowledge Script parameters in a separate filter file.

In many cases, specifying a filter file provides greater flexibility and makes modifying your search criteria most straightforward because you can add virtually any number of expressions and you do not need to modify the Knowledge Script properties through the Operator Console to pick up your changes.

If you want to use a filter file:

- Identify the strings that you want to find a match for in the syslog file (the entries you want to include in your results).
- Create the file with one regular expression string per line to locate matching strings.
- Make sure the file exists on the target UNIX computer.
- Type the absolute path to the file on the local UNIX agent in the **Optional file containing additional filters** parameter and start the job.

SystemUpTime

Use this Knowledge Script to monitor the system up time for a UNIX server. This Knowledge Script tracks the number of hours that the computer has been operational since it was last rebooted. If the computer was rebooted within the monitoring interval, an event is raised.

Resource Object

UNIX computer icon

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. If set to y, the script returns the number of hours the system has been up. The default is n.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.

TopCpuProcs

Use this Knowledge Script to monitor the total CPU resources used by all processes and which processes consume the most CPU resources. If the CPU usage for any of the listed processes exceeds the threshold you set, an event is raised.

Resource Objects

CPU folder.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for charts and reports. If set to y, the script returns the total CPU usage for the interval and the detail message lists the processes consuming the most CPU resources. The default is n.
Maximum CPU usage (%) for all processes threshold	Enter a threshold for the maximum percentage of CPU resources that should be in use for all processes. The default is 90%.
Number of top processes to display (0 means all)	Specify the number of top processes you want displayed in the detail message (event or data). Enter 0 if you want all processes displayed. The default is 5 processes. **Note** It is recommended that you limit the number of processes included in the detail message to the top five to ten processes, rather than reporting on all processes. In most cases, including all processes increases the size of the detail message without providing you with more useful information. Typically, the top few processes are the most significant and the most likely ones you are looking to track down for troubleshooting purposes.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

TopMemoryProcs

Use this Knowledge Script to monitor the system memory usage to identify which processes are consuming the most memory. This Knowledge Script raises an event if the virtual or physical memory usage for the system crosses the threshold you specify. The top number of processes that are consuming the most physical memory are reported in the event and data detail messages.

Resource Object

Memory folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Specify whether you want to raise an event if the memory usage for all processes crosses the threshold you specify. The default is y.
Collect virtual memory data? (y/n)	Specify whether you want to collect information on virtual memory usage for charts and reports. If set to y, this script returns the virtual memory usage for the interval and the detail message lists the processes consuming the most memory resources. The default is n.
Collect physical memory data?	Specify whether you want to collect information on physical memory usage for charts and reports. If set to y, this script returns the physical memory usage for the interval and the detail message lists the processes consuming the most memory resources. The default is n.
Maximum virtual memory used (%) threshold	Type a threshold for the maximum percentage (%) of virtual memory that should be in use. The default is 90%.
Maximum physical memory used (%) threshold	Type a threshold for the maximum percentage (%) of physical memory that should be in use for all processes. Physical memory not being used by processes is often used dynamically by the system as cache. The default is 100%.
Number of top processes to display (0 means all)	Type a number indicating how many top processes you want AppManager to display in the detail message (event or data). Type 0 if you want all processes recorded in the detail message. The default is 5. **Note** In most cases, including all processes increases the size of the detail message without providing you with more useful information. Therefore, NetIQ recommends that you limit the number of processes included in the detail message to the top five or ten processes. Typically, the top few processes are the most significant for troubleshooting purposes. Processes that share memory appear to be using more memory than they actually are.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Description	How to Set It
HPUX: Include reserved value in calculations?	Specify whether you want to include reserved swap space in the calculations. If set to y, calculations will include space reserved system for deactivation and paging processes. This parameter is only available on computers running the HP-UX operating system. The default is y.
HPUX: Include memory pseudo-swap values in calculations?	Specify whether you want to include pseudo-swap space in the calculations. Pseudo-swap space might be up to 3/4 of the available system memory. If set to y, calculations will include space in the pseudo swap reservation counters. This parameter is only available on computers running the HP-UX operating system. The default is y.

ZombieProcs

Use this Knowledge Script to detect the number of zombie processes currently left waiting to be cleaned up. If the number of zombie processes exceeds the threshold you set, an event is raised. A large or increasing number of zombie processes can indicate a program you are running is launching child processes but not properly terminating either the parent or child process, or that you may need to exit a running program to eliminate the zombie processes.

Resource Object

CPU folder

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if over the threshold?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, the script returns the number of zombie processes detected for the interval. The default is n.
Maximum number of zombie processes threshold	Enter a threshold for the maximum number of zombie processes waiting in the interval. The default is 10 zombie processes.
Event severity level	Set the event notification level, from 1 to 40, to indicate the importance of each event. By default, the severity level is 5.

Chapter 69
VMware VirtualCenter Knowledge Scripts

AppManager for VMware provides the following Knowledge Scripts for monitoring VMware vCenter, VMware ESX Server hosts, VMware datastores, and VMware virtual machines, also called guests. The scripts can also monitor vCenter alarms, events, and task failures. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
Alarms	Monitors vCenter alert and warning alarms and raises AppManager events when those vCenter alarms get triggered.
ClusterCPUusage	Monitors the CPU usage of the cluster.
ClusterMemUsage	Monitors memory usage, memory swap used, and memory balloon for a cluster.
ClusterStatus	Monitors the configuration status of the cluster.
Configuration	Use this Knowledge Script to generate an inventory of all hosts and virtual machines for the selected vCenter as well as configuration details for each.
ConfigureHostTraffic	Enables an SNMP firewall port for a given host.
DatastoreUsage	Monitors the vCenter datastore usage.
Events	Monitors vCenter error, warning, and informational events, and raises AppManager events when those vCenter events occur.
HostConnected	Monitors changes in the connection status of hosts to the vCenter. For example, this script monitors whether the host is visible to the vCenter.
HostCPUUsage	Monitors the percentage of host CPU usage and CPU Used.
HostDataStoreUsage	Monitors datastore usage for a host.
HostDiskIO	Monitors disk reads/writes for a host.
HostDiskTotalLatency	Monitors and collects data for host total disk latency performance metrics.
HostMemoryUsage	Monitors memory usage, memory swap used, and memory balloon for a host.
HostNetworkIO	Monitors network reads/writes for a host.
HWCorrectableMemCondition	Monitors the state of the correctable memory condition.
HWFanStatus(CPU)	Monitors the state of the CPU fan.
HWFanStatus(System)	Monitors the state of the system fan.
HWHPNICLost	For HP ESX hosts only, monitors for SNMP trap messages that indicate the Failed status of a logical adapter.

Knowledge Script	What It Does
HWHPNICRestorScripted	For HP ESX hosts only, monitors for SNMP trap messages that indicate the Restored status of a logical adapter.
HWLogicalDiskStatus	Monitors the state of a logical disk.
HWPhysicalDiskStatus	Monitors the state of a physical disk.
HWPowerSupply	Monitors the condition of the power supply in the system.
HWThermalStatus	Monitors the thermal state of the system.
ResourcePoolCPUusage	Monitors the CPU usage of the resource pool.
ResourcePoolMemUsage	Monitors memory usage and memory balloon for the resource pool.
ResourcePoolStatus	Monitors the overall status of the Resource pool.
ServiceHealthCheck	Monitors vCenter Server services.
Tasks	Raises AppManager events when monitored vCenter task failures occur.
VirtualCenterCPUUsage	Monitors the CPU usage of the vCenter process and the CPU usage on the computer hosting vCenter
VirtualCenterMemoryUsage	Monitors memory usage of the vCenter process and total memory usage on the computer hosting vCenter
VirtualMachineInventory	Monitors virtual machines that are added, removed, renamed, or migrated within vCenter.
VmConnected	Monitors changes in the connection status of virtual machines to the vCenter.
VmCPUusage	Monitors CPU usage, CPU ready, CPU wait, and CPU used for a virtual machine.
VmDiskIO	Monitors disk reads/writes for a virtual machine.
VmDiskUsage	Monitors logical disk usage for a virtual machine.
VmMemoryUsage	Monitors memory usage, memory consumed, and memory balloon for a virtual machine.
VmNetworkIO	Monitors network reads/writes for a virtual machine.
VmPowerStatus	Monitors changes in the power status of virtual machines.
VmToolsStatus	Monitors the tools status of virtual machines.
VirtualCenter_RPT_VCConfiguration	Generates a report about the vCenter host, virtual machine configuration, and number of hosts configured per vCenter Server.
VirtualCenter_RPT_VCCPUUsage	Generates a report about the CPU usage of all hosts. This script also compares CPU usage of all virtual machines on a host.
VirtualCenter_RPT_VCHostDataStoreUsage	Generates a report to compare host datastore usage.
VirtualCenter_RPT_VCMemoryUsage	Generates a report to compare memory usage of all hosts.
VirtualCenter_RPT_VCNetworkIO	Generates a report to compare network I/O of all hosts.
Recommended Knowledge Script Groups	Performs essential monitoring of your vCenter environment.

Alarms

Use this Knowledge Script to monitor vCenter *alarms*, which are actions that are triggered when a condition or set of conditions occurs within vCenter. A default set of alarms is defined for vCenter, but vCenter administrators can also define custom alarms.

This script raises an event when monitored vCenter alarms are triggered. You can filter the vCenter alarms by alarm type and alarm name. Use the Objects tab to define the resources you want to monitor.

In addition, you can use the Alarms Knowledge Script to monitor changes to your ESX hardware. For more information, see "Using the Alarms Script to Monitor ESX Hardware" on page 3932.

Each event report shows the following information:

- Target
- Category
- Description
- User name
- Time on the vCenter Server when the alarm occurred

Notes

- The structure of the vCenter Web Service architecture allows you to run only *one* Alarms job on a specific vCenter Server at a time. This limitation prevents the user from starting multiple jobs that monitor the same alarms, which would increase the load on the vCenter Server without any real monitoring benefit. If you have an Alarms job running and try to start another Alarms job, the second job will not complete, and an event message will be raised.
- To avoid long delays when running other VMware Knowledge Scripts, you should only run the Alarms script if your AppManager agent is running on the vCenter server, and not in proxy mode.
- The first time you run this script, you may experience a short delay before actual monitoring begins. This delay is caused by the various initialization processes that must be carried out by the Alarms script.

Resource Objects

Run the Discovery_VirtualCenter Knowledge Script on the objects you want to monitor before running this Knowledge Script. You can also monitor objects that the Discovery_VirtualCenter Knowledge Script does *not* discover, such as distributed virtual port groups and distributed virtual switches.

- vCenter server
- Clusters
- Datacenters
- Datastores
- Hosts
- Resource pools
- Virtual machines
- Folders (you can only monitor the folder objects found under the Host & Clusters parent folder in the TreeView pane)
- Distributed virtual port groups (not displayed in the TreeView pane)

- Distributed virtual switches (not displayed in the TreeView pane)
- Network (not displayed in the TreeView pane)

Default Schedule

The default interval for this script is **Asynchronous**. Regardless of the schedule you select, once you start the Knowledge Script, its job status appears as **Running**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when AppManager fails to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot log in to vCenter. The default is 5.
Event severity when Alarms job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Alarms job fails. The default is 5.
Event severity when filter settings contain conflicts	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the filter settings contain conflicts. The default is 15.
Additional Settings	
Event Details	
Event detail format	Select **HTML Table** or **Plain Text** as the format for the detail in an event message. The default is HTML Table.
Monitor vCenter Alarms	
Event Notification	
Raise event if vCenter alert alarm is triggered?	Set to **Yes** to raise an event if a vCenter alert alarm that matches your criteria is triggered. The default is Yes.
Event severity when vCenter alert alarm is triggered	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a vCenter alert alarm is triggered. The default is 5.
Alarm name	If you want to raise events on specific alarms, provide the names of the vCenter alarms you want to monitor. AppManager raises an event when an alarm matching your type, name, and status criteria is triggered. If you do not enter an alarm name, AppManager raises events for all alert alarms. The asterisk (*) and (?) are acceptable wildcards. Separate multiple names with a comma, without any spaces.
Also raise events on unassociated TreeView objects?	Select **Yes** to raise an event for unassociated objects in the TreeView pane. The default is unselected.
Raise event if vCenter warning alarm is triggered?	Set to **Yes** to raise an event if a vCenter warning alarm that matches your criteria is triggered. The default is Yes.
Event severity when vCenter warning alarm is triggered	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a vCenter warning alarm is triggered. The default is 15.

Parameter	How to Set It
Alarm name	If you want to raise events on specific alarms, provide the names of the vCenter alarms you want to monitor. AppManager raises an event when an alarm matching your type, name, and status criteria is triggered. If you do not enter an alarm name, AppManager raises events for all warning alarms. The asterisk (*) and (?) are acceptable wildcards. Separate multiple names with a comma, without any spaces.
Also raise events on unassociated TreeView objects?	Select **Yes** to raise an event for unassociated objects in the TreeView pane. The default is unselected.

Using the Alarms Script to Monitor ESX Hardware

You can use the Alarms Knowledge Script to monitor state changes in your ESX hardware, such as when a fan in a group of fans is close to overheating. Before you can monitor your hardware with the Alarms script, you need to create the hardware alarms in vCenter.

System requirements for monitoring ESX hardware:

- At minimum, VMware vCenter 4.0
- At minimum, ESX 3.5, Update 4, or ESXi 4.0 on the ESX servers you want to monitor.

To create a custom alarm in vCenter:

1. In vCenter, locate the ESX server you want to monitor in the left pane.
2. On the Hardware Status tab, identify the hardware element you want to monitor, such as a fan group.
3. On the Alarms tab, verify that the **Definitions** view is selected.
4. Right-click anywhere on the Alarms tab and select **New Alarm**.
5. In the Alarm Settings dialog box, type an alarm name, such as `All Fans - Status Yellow`.

   Note
   Make a note of this name, as you will need to type this name into the Alarms Knowledge Script in AppManager when you run the Alarms script.

6. Type a short description of the alarm, such as `Alarm triggered when any Host's fan has a status of Yellow.`
7. From the Monitor list, select **Hosts**.
8. Select **Monitor for specific events occurring on this object**.
9. Verify that **Enable this alarm** is checked.
10. On the Triggers tab, click **Add**.
11. From the Event list, select the relevant event type, such as **Hardware Health Changed**.
12. From the Status list, select the relevant alarm status, such as **Alert** or **Warning**.
13. In the Conditions field, click **Advanced**.
14. In the Trigger Conditions dialog box, specify the different Argument > Operator > Value combinations that must be present to set off the alarm. For example, **newgroup > equal to > Fan** and **newState > equal to > Yellow**.

    Note
    The newGroup argument represents the sensor being monitored, such as Fan or Voltage. The newState argument represents the current state of the sensor in the newGroup argument.

15. Click **OK** to close the Trigger Conditions dialog box.
16. Click **OK** to close the Alarms Settings dialog box. The custom alarm is now set up in vCenter, and you can start monitoring that alarm with AppManager.

To set up the Alarms script to monitor the new custom alarm in vCenter:

1. In AppManager, run the Alarms Knowledge Script on the vCenter object you want to monitor for ESX hardware alarms.
2. Click the **Values** tab.
3. ***If you set up a vCenter alert alarm in the previous procedure,*** type the alert alarm name, such as `All Fans - Status Yellow`, into the *Alarm name* parameter under the *Raise event if vCenter alert alarm is triggered?* parameter.
4. ***If you set up a vCenter warning alarm in the previous procedure,*** type the warning alarm name, such as `All Fans - Status Red`, into the *Alarm name* parameter under the *Raise event if vCenter warning alarm is triggered?* parameter.
5. Select **Yes** for the relevant *Raise event* parameter.
6. Set the severity level in the relevant *Event severity* parameter.
7. Click **OK** to run the script.

Note
Closing the AppManager Alarms event will not clear the alarm event in vCenter, and closing the vCenter alarm will not clear the AppManager Alarms event.

ClusterCPUusage

Use this Knowledge Script to monitor the CPU usage of the cluster. This script raises an event if CPU usage exceeds the threshold you set. In addition, this script generates data streams for CPU usage. This script monitors and collects data for the following performance metrics:

- CPU usage as a percentage: the sum of actively used CPU of all virtual machines in the cluster, as a percentage of the total available CPU.
- CPU usage in MHz: the sum of actively used CPU of all virtual machines in the cluster, in megahertz.

Prerequisite

To enable the Knowledge Script to collect accurate CPU usage data, set the following **Statistics Collection Intervals** appropriately in the vCenter Management Server Configuration:

- **Collection Frequency**: The interval duration in vCenter must be less than or equal to the AppManager job interval schedule. For example, if you run the ClusterCPUUsage Knowledge Script at 15-minute intervals, the interval duration in vCenter must be less than or equal to 15 minutes.

For more information about setting the Interval Duration and Statistics Level in the vCenter, see the VMware Virtual Infrastructure 3 documentation.

Resource Object

vCenter-monitored clusters

Default Schedule

By default, this script runs every **15 minutes**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when percent CPU Usage exceeds the threshold?	Select **Yes** to raise an event if percent CPU usage exceeds the threshold you set. The default is unselected.
Event severity when percent CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which percent CPU usage exceeds the threshold. The default is 15.
Raise event when CPU usage in MHz exceeds the threshold?	Select **Yes** to raise an event if CPU usage in MHz exceeds the threshold you set. The default is Yes.
Event severity when CPU usage in MHz exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage in MHz exceeds the threshold. The default is 15.

Parameter	How to Set It
Raise event when cluster is either removed or has configuration issues?	Select **Yes** to raise an event if when cluster is either removed or has configuration issues. The default is Yes.
Event severity when cluster is either removed or has configuration issues	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the cluster is either removed or has configuration issues. The default is 15.
Event severity when failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when the ClusterCPUusage job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ClusterCPUUsage job fails unexpectedly. The default is 5.
Data Collection	
Collect data for percent CPU usage?	Select **Yes** to collect percent CPU usage data for charts and reports. The default is unselected.
Collect data for CPU usage in MHz?	Select **Yes** to collect CPU usage data in MHz for charts and reports. The default is unselected.
Monitoring	
Maximum threshold for CPU usage	Specify the maximum amount of CPU usage that can occur before an event is raised. The default is 80 percent.
Maximum threshold for CPU usage	Specify the maximum amount of CPU usage that can occur before an event is raised. The default is 800 MHz.

ClusterMemUsage

Use this Knowledge Script to monitor the memory usage of the cluster. This script raises an event when a monitored value exceeds the threshold you set. This script monitors and collects data for the following performance metrics:

- Memory active: the amount of host machine memory used by all powered-on virtual machines in the cluster. A cluster's consumed memory consists of virtual machine consumed memory and overhead memory. It does not include host-specific overhead memory, such as memory used by the service console or VMkernel.
- Memory balloon: the amount of memory allocated by the virtual machine memory control driver, which is installed with VMware Tools.
- Memory granted: the amount of memory (in kilobytes) that has been allocated to virtual machines running on all hosts in the cluster.
- Memory swap used: the sum of the memory swapped by the powered-on virtual machines on all hosts in the cluster.
- Memory usage: the amount of total configured memory available for use.

Prerequisite

To enable the Knowledge Script to collect accurate memory related data, set the following **Statistics Collection Intervals** appropriately in the vCenter Management Server Configuration:

- **Collection Frequency**: The interval duration in vCenter must be less than or equal to the AppManager job interval schedule. For example, if you run the ClusterMemUsage Knowledge Script at 15-minute intervals, the interval duration in vCenter must be less than or equal to 15 minutes.

For more information about setting the Interval Duration and Statistics Level in the vCenter, see the VMware Virtual Infrastructure 3 documentation.

Resource Object

vCenter-monitored clusters

Default Schedule

By default, this script runs every **15 minutes**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when memory active exceeds the threshold?	Select **Yes** to raise an event when memory active exceeds the threshold you set. The default is unselected.
Event severity when memory active exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory active exceeds the threshold. The default is 15.
Raise event when memory balloon used exceeds the threshold?	Select **Yes** to raise an event when memory balloon used exceeds the threshold you set. The default is Yes.
Event severity when memory balloon used exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory balloon used exceeds the threshold. The default is 15.
Raise event when memory granted exceeds the threshold?	Select **Yes** to raise an event when memory granted exceeds the threshold you set. The default is unselected.
Event severity when memory granted exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory granted exceeds the threshold. The default is 15.
Raise event when memory swap used exceeds the threshold?	Select **Yes** to raise an event when memory swap used exceeds the threshold you set. The default is Yes.
Event severity when memory swap used exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory swap used exceeds the threshold. The default is 15.
Raise event when memory usage exceeds the threshold?	Select **Yes** to raise an event when memory usage exceeds the threshold you set. The default is Yes.
Event severity when memory usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. The default is 15.
Raise event when cluster is either removed or has configuration issues?	Select **Yes** to raise an event when the cluster is either removed or has configuration issues. The default is Yes.
Event severity when cluster is either removed or has configuration issues	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the cluster is either removed or has configuration issues. The default is 15.
Event severity when failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when ClusterMemUsage job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ClusterMemUsage job fails unexpectedly. The default is 5.
Data Collection	
Collect data for memory active?	Select **Yes** to collect cluster memory usage data for charts and reports. The default is unselected. **Note** Because VMware permits over-allocation of resources, it is possible for data collection to return cluster memory usage data points in excess of 100 percent.

Parameter	How to Set It
Collect data for memory balloon used?	Select **Yes** to collect cluster memory balloon used data for charts and reports. The default is unselected. **Note** Because VMware permits over-allocation of resources, it is possible for data collection to return cluster memory balloon data points in excess of 100 percent.
Collect data for memory granted?	Select **Yes** to collect cluster memory granted data for charts and reports. The default is unselected.
Collect data for memory swap used?	Select **Yes** to collect cluster memory swap data for charts and reports. The default is unselected. **Note** Because VMware permits over-allocation of resources, it is possible for data collection to return cluster memory swap data points in excess of 100 percent.
Collect data for memory usage?	Select **Yes** to collect cluster memory usage data for charts and reports. The default is unselected. **Note** Because VMware permits over-allocation of resources, it is possible for data collection to return cluster memory usage data points in excess of 100 percent.
Monitoring	
Maximum threshold for memory active	Specify the maximum percentage of cluster memory active that can occur before an event is raised. The default is 20 percent.
Maximum threshold for memory usage	Specify the maximum percentage of cluster memory usage that can occur before an event is raised. The default is 80 percent.
Maximum threshold for memory balloon used	Specify the maximum percentage of cluster memory balloon that can occur before an event is raised. The default is 20 percent.
Maximum threshold for memory granted	Specify the maximum percentage of cluster memory granted that can occur before an event is raised. The default is 1024 megabytes.
Maximum threshold for memory swap used	Specify the maximum percentage of cluster memory swap used that can occur before an event is raised. The default is 20 percent.

ClusterStatus

Use this Knowledge Script to monitor the configuration status of the cluster. This script raises an event if the state of the cluster changes. In addition, this script generates data streams for overcommitted state, overcommitted state, and inconsistent state.

Resource Object

vCenter-monitored clusters

Default Schedule

By default, this script runs every **15 minutes**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when cluster state changes?	Select **Yes** to raise an event if the state of the cluster changes. The default is Yes.
Event severity when cluster state inconsistent	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the cluster state changes to inconsistent. The default is 5.
Event severity when cluster state overcommitted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the cluster state changes to overcommitted. The default is 15.
Event severity when cluster state undercommitted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the cluster state changes to undercommitted. The default is 25.
Event severity when failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when ClusterStatus job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ClusterStatus job fails unexpectedly. The default is 5.

Parameter	How to Set It
Data Collection	
Collect data for status change?	Select **Yes** to collect data about cluster status for charts and reports. The default is unselected. **Note** If enabled, data collection returns the following data: 100 for undercommitted state, 50 for overcommitted state, and 0 for inconsistent state.

Configuration

Use this Knowledge Script to generate an inventory of all hosts and virtual machines for the selected vCenter environment as well as configuration details for each host and virtual machine.

Note
This script may take more than an hour to run on environments with more than 500 virtual machines.

Each host report shows the following information:

General information

- Type
- Version
- Build
- System manufacturer
- System model
- Number of processors and resources of each (in GHz)
- Processor type
- Total CPU resources (in GHz)
- Memory (in megabytes)
- Number of virtual machines
- If VMotion is enabled or disabled
- Date and time the system was booted
- System date and time
- Uptime

Processor information

- Processor type
- Processor speed
- Number of processor sockets
- Number of cores per socket
- Number of logical processors
- If hyperthreading is enabled or disabled

Memory information

- Total RAM (in megabytes)
- RAM in use by virtual machines
- Service console RAM (in megabytes)

Storage information

- Number of datastores
- Table of, device, capacity (in gigabytes), free space (in gigabytes), and type

- Table of adapters, device, host bus adapter, type, and SAN identifier
- Table of physical adapters, device, speed, vSwitch, and WOL support
- Table of Virtual switches, configured ports, and available ports

Virtual machine and template information

- Table of virtual machines, state, uptime, CPU count, memory (in megabytes), guest OS, and notes
- Table of templates, CPU count, memory (in megabytes), guest OS, and notes

For each virtual machine, the report shows the following information:

General information

- DNS name
- Guest operating system
- Template
- State
- Uptime
- Host machine
- VMware tools status
- VMware tools version
- Number of snapshots

CPU information

- Number of CPUs
- CPU reservation (in MHz)

Memory information

- Memory (in megabytes)
- Memory reservation (in megabytes)

Disk information

- Table of disks, their type, and their size (in gigabytes)

Network information

- Table of network interface cards, VLAN, emulation, IP address, and MAC address

Resource Object

vCenter

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameter as needed:

Parameter	How to Set It
Event Notification	
Raise event when configuration files successfully generated?	Select **Yes** to raise an event if the report is successfully generated. The default is Yes.
Event severity when configuration files successfully generated	Set the event severity level, from 1 to 40, to indicate the importance of an event in which configuration files are generated successfully. The default is 25.
Event severity when failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when Configuration job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Configuration job fails unexpectedly. The default is 5.
Knowledge Script Settings	
Full path to output folder for result files	Provide the path to a location on the agent computer in which to save the configuration. The default path is C:\ProgramFiles\NetIQ\Temp\NetIQ_Debug\VMware
Report file name	Provide a file name for the report. The default name is default.html

ConfigureHostTraffic

Use this Knowledge Script to enable firewalls on host ESX servers to allow SNMP traffic. This script raises an event if the operation succeeds or fails. This Knowledge Script replaces the EnableSNMPTraffic Knowledge Script.

Prerequisite

Enable the **Security Profile and Firewall** permission to run this Knowledge Script. For more information, see "Configuring vCenter Connection Credentials" on page 10.

Resource Object

vCenter-monitored host. For example, ESX server.

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when host does not support firewall configuration?	Select **Yes** to raise an event when a host does not support firewall configuration. The default is Yes.
Event severity when host does not support firewall configuration	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a host does not support firewall configuration. The default is 15.
Event severity when host server no longer connected to VirtualCenter	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the selected host server has been removed from vCenter. The default is 35.
Event severity failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when ConfigureHostTraffic job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ConfigureHostTraffic job fails unexpectedly. The default is 5.
Host inbound traffic settings	
Enable SNMP traffic?	Select **Yes** to raise an event when the SNMP inbound traffic is enabled successfully. The default is Yes.
Event severity when SNMP inbound traffic enabled successfully	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMP inbound traffic is enabled successfully. The default is 25.

Parameter	How to Set It
Event severity when SNMP inbound traffic is already enabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which inbound traffic is already enabled. The default is 35.
Event severity when SNMP inbound traffic failed to be enabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SNMP inbound traffic failed to be enabled. The default is 5.

DatastoreUsage

Use this Knowledge Script to monitor datastore usage. This script raises an event if the amount of available datastore free space exceeds the threshold and the percentage of datastore used falls below the threshold. In addition, this script generates data streams for gigabytes or megabytes of available free space and for the percentage of datastore used.

Resource Object

vCenter-monitored Datastore

Default Schedule

By default, this script runs every **three hours**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on datastore utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when available free space falls below the threshold?	Select **Yes** to raise an event if the amount of available datastore free space falls below the threshold you set. The default is Yes.
Event severity when available free space falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of available datastore free space falls below the threshold. The default is 15.
Raise event when datastore percentage used exceeds the threshold?	Select **Yes** to raise an event if the percentage of datastore used exceeds the threshold you set. The default is Yes.
Event severity when percentage used exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance an event in which the percentage of datastore used exceeds the threshold. The default is 15.
Raise event when datastore is either inactive or removed?	Select **Yes** to raise an event if datastore is either inactive or removed. The default is Yes.
Event severity when datastore is either inactive or removed	Set the event severity level, from 1 to 40, to indicate the importance an event in which datastore is either inactive or removed. The default is 15.
Event severity when failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve datastore metrics from vCenter. The default is 15.
Event severity when failed to log in	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.

Parameter	How to Set It
Event severity when DataStoreUsage job fails unexpectedly	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DataStoreUsage job fails unexpectedly. The default is 5.
Data Collection	
Collect data for free space?	Select **Yes** to collect data about the amount of free space for charts and reports. The default is unselected. **Note** This script does not create new data streams when the free space unit is changed. For example, if you change the unit of measure for this parameter from megabytes to gigabytes, the script should generate a new data stream in gigabytes, but the job continues to collect data on data streams in megabytes.
Collect data for percentage used?	Select **Yes** to collect data about the percentage of datastore used for charts and reports. The default is unselected.
Monitoring	
Minimum threshold for datastore free space	Specify the minimum amount of datastore free space that must be available to prevent an event from being raised. The default is 500. Use the *Select datastore free space unit* parameter to select **GBytes** or **MBytes** as the unit of measure for free space.
Select datastore free space unit	Select whether to measure the amount of datastore free space in **GBytes** or **MBytes**. The default is GBytes.
Maximum threshold for datastore space used percentage	Specify the maximum percentage of datastore that can be used before an event is raised. The default is 90%.

Events

Use this Knowledge Script to monitor events reported by vCenter Server, such as when a user powers off a virtual machine. You can filter the events by vCenter entity type, user name, and event description. This Knowledge Script raises an event based on these filters. Use the Objects tab to define the resources you want to monitor. This script monitors all error and warning type events by default.

Warning

This Knowledge Script can potentially raise an excessive number of AppManager events, as well as unassociated events for objects not discovered in the AppManager TreeView pane. Use the filtering parameters in this script, such as event description and entity type, to limit the number of events monitored by the script and prevent a flood of irrelevant vCenter events.

Each event report shows the following information:

- Target
- Category
- Description
- User name
- Time on the vCenter Server when the event occurred

Notes

- The structure of the vCenter Web Service architecture allows you to run only *one* Events job on a specific vCenter Server at a time. This limitation prevents the user from starting multiple jobs that monitor the same events, which would increase the load on the vCenter Server without any real monitoring benefit. If you have an Events job running and try to start another Events job, the second job will not complete, and an event message will be raised.
- To avoid long delays when running other VMware Knowledge Scripts, you should only run the Events script if your AppManager agent is running on the vCenter server, and not in proxy mode.
- The first time you run this script, you may experience a short delay before actual monitoring begins. This delay is caused by the various initialization processes that must be carried out by the Events script.

Resource Objects

Run the Discovery_VirtualCenter Knowledge Script on the objects you want to monitor before running this Knowledge Script. You can also monitor objects that the Discovery_VirtualCenter Knowledge Script does *not* discover, such as distributed virtual port groups and distributed virtual switches.

- vCenter server
- Clusters
- Datacenters
- Datastores
- Hosts
- Resource pools
- Virtual machines
- Folders (you can only monitor the folder objects found under the Host & Clusters parent folder in the TreeView pane)

- Distributed virtual port groups (not displayed in the TreeView pane)
- Distributed virtual switches (not displayed in the TreeView pane)

Default Schedule

The default interval for this script is **Asynchronous**. Regardless of the schedule you select, once you start the Knowledge Script, its job status appears as **Running**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when AppManager failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in. The default is 5.
Event severity when Events job fails unexpectedly	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager fails unexpectedly. The default is 5.
Event severity when filter settings contain conflicts	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the filter settings contain conflicts. The default is 15.
Additional Settings	
Event Details	
Event detail format	Select either **HTML Table** or **Plain Text** as the format for event detail. The default is HTML Table.
Monitor vCenter Events	
Event Notification	
Raise event if vCenter "error" event is detected?	Select **Yes** to raise an event if an "error" event is detected. The default is Yes.
Event severity if vCenter "error" event is detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which a vCenter "error" is detected. The default is 5.
Select vCenter entity type(s)	Click **Browse [...]** to select the vCenter entity type you want to monitor. The default is all entity types: Datacenter,Datastore,Cluster,Folder,HostSystem,ResourcePool,VirtualMachine.
User	If you want to raise events only for a specific user, provide the name of the vCenter user you want to monitor. If you do not enter a user name, AppManager raises events related to all users. The asterisk (*) and (?) are acceptable wildcards. **Note** You must enter at least a (*) for this script to run. Do not leave this parameter blank.
Event description	If you want to raise events that include specific text, provide text the event description must contain to be monitored. If you do not provide text, AppManager raises events regardless of text. The asterisk (*) and (?) are acceptable wildcards. **Note** You must enter at least a (*) for this script to run. Do not leave this parameter blank.
Also raise events on unassociated TreeView objects?	Select **Yes** to raise an event for unassociated objects in the TreeView pane. The default is unselected.

Parameter	How to Set It
Raise event if vCenter “warning” event is detected?	Select **Yes** to raise an event if a vCenter “warning” event is detected. The default is Yes.
Event severity when vCenter “warning” event is detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which a vCenter “warning” is detected. The default is 15.
Select vCenter entity type(s)	Click **Browse [...]** to select the vCenter entity type you want to monitor. The default is all entity types: Datacenter,Datastore,Cluster,Folder,HostSystem,ResourcePool,VirtualMachine.
User	If you want to raise events only for a specific user, provide the name of the vCenter user you want to monitor. If you do not enter a user name, AppManager raises events related to all users. The asterisk (*) and (?) are acceptable wildcards. **Note** You must enter at least a (*) for this script to run. Do not leave this parameter blank.
Event description	If you want to raise events only that include specific text, provide text the event description must contain to be monitored. If you do not provide text, AppManager raises events regardless of text. The asterisk (*) and (?) are acceptable wildcards. **Note** You must enter at least a (*) for this script to run. Do not leave this parameter blank.
Also raise events on unassociated TreeView objects?	Select **Yes** to raise an event for unassociated objects in the TreeView pane. The default is unselected.
Raise event if vCenter “info” event is detected?	Select **Yes** to raise an event if a vCenter “info” event is detected. The default is unselected.
Event severity when vCenter “info” event is detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which a vCenter “info” message is detected. The default is 25.
Select vCenter entity type	Click **Browse [...]** to select the vCenter entity type you want to monitor. The default is all entity types: Datacenter,Datastore,Cluster,Folder,HostSystem,ResourcePool,VirtualMachine.
User	If you want to raise events only for a specific user, provide the name of the vCenter user you want to monitor. If you do not enter a user name, AppManager raises events related to all users. The asterisk (*) and (?) are acceptable wildcards. **Note** You must enter at least a (*) for this script to run. Do not leave this parameter blank.
Event description	If you want to raise events only that include specific text, provide text the event description must contain to be monitored. If you do not provide text, AppManager raises events regardless of text. The asterisk (*) and (?) are acceptable wildcards. **Note** You must enter at least a (*) for this script to run. Do not leave this parameter blank.
Also raise events on unassociated TreeView objects?	Select **Yes** to raise an event for unassociated objects in the TreeView pane. The default is unselected.
Data Collection	**Note** This script can only collect data for those event categories for which you have selected Yes for the relevant *Raise event for...* parameter. For example, if you want to collect data for error events, you must select **Yes** for the *Raise event if vCenter “error” event is detected?* parameter.
Default time interval to collect data	Specify a default time interval for collecting data for charts and reports. The default is 5.

Parameter	How to Set It
Collect data for error events?	Select **Yes** to collect data about error events for charts and reports. The default is Yes.
Collect data for warning events?	Select **Yes** to collect data about warning events for charts and reports. The default is unselected.
Collect data for info events?	Select **Yes** to collect data about informational events for charts and reports. The default is unselected.

HostConnected

Use this Knowledge Script to monitor changes in the connection status of hosts to vCenter, such as when a host is connected to the vCenter server or when a host goes into maintenance mode from normal mode.

This script raises an event if a host is disconnected or reconnected, or if a host goes into or comes out of maintenance mode. This script will not generate host disconnect or reconnect events while the host is in maintenance mode.

Resource Object

vCenter-monitored host. For example, ESX server.

Default Schedule

By default, this script runs every **15 minutes**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event when host is removed?	Select **Yes** to raise an event when a host is removed. The default is unselected.
Event severity when host is removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a host is removed. The default is 15.
Event severity when failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when HostConnected job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HostConnected job fails unexpectedly. The default is 5.
Additional Settings	
Event Details	
Event detail format	Select either **HTML Table** or **Plain Text** as the format for event detail. The default is HTML Table.
Monitor Connection Status	
Event Notification	

Parameter	How to Set It
Raise event when host enters disconnected state?	Select **Yes** to raise an event when a host enters a disconnected state. The default is Yes. **Note** The script will not generate disconnect events if the host is in maintenance mode.
Event severity when host enters disconnected state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a host enters a disconnected state The default is 15.
Raise event when host is in maintenance mode?	Select **Yes** to raise an event when a connected host goes into maintenance mode. The default is Yes.
Event severity when host in maintenance mode	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a host goes into maintenance mode. The default is 15.
Raise event when host is out of maintenance mode?	Select **Yes** to raise an event when a connected host comes out of maintenance mode. The default is Yes.
Event severity when host out of maintenance mode	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a host comes out of maintenance mode. The default is 15.
Raise event when host enters connected state?	Select **Yes** to raise an event when a host enters a connected state. The default is Yes. **Note** The script will not generate reconnect events if the host is in maintenance mode.
Event severity when host enters connected state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a host enters a connected state. The default is 15.
Data Collection	
Collect data for host availability?	Select **Yes** to collect host availability data for charts and reports. When enabled, data collection returns 100 when a host is available and 0 when a host is unavailable. The default is unselected.
Collect data for host connectivity?	Select **Yes** to collect host connectivity data for charts and reports. When enabled, data collection returns 100 when a host is connected and 0 when a host is not connected. The default is unselected.

HostCPUUsage

Use this Knowledge Script to monitor host CPU usage and CPU used. This script raises an event if CPU usage exceeds the threshold you set. This script monitors the following metrics:

- CPU reserved capacity - Total CPU capacity reserved by the virtual machines.
- CPU usage - Actively used CPU of the host, as a percentage of the total available CPU reserved by virtual machines running on this host.
- CPU usage in MHz - Total amount of CPU used, in MHz, during the interval.
- CPU used - Sum of the actively used CPU of all powered on virtual machines on a host.

If this script is running in addition to the Disk I/O, Memory usage, or Network I/O scripts, you should instead run the HostCPUUsage, HostMemoryUsage, HostDiskIO, and HostNetworkIO Knowledge Scripts to optimize the resource usage on the host.

Note
When a host goes into maintenance mode all host scripts, except for the HostConnected Knowledge Script, suppress events and data.

Resource Object

vCenter-monitored host. For example, ESX server.

Default Schedule

By default, this script runs every **15 minutes**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event when CPU metrics are not available?	Select **Yes** to raise an event when CPU metrics are not available. The default is Yes.
Event severity when CPU metrics are not available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU metrics are not available. The default is 15.
Raise event when host is either disconnected or removed?	Select **Yes** to raise an event when host is either disconnected or removed. The default is Yes.
Event severity when host is either disconnected or removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the host is either disconnected or removed. The default is 15.

Parameter	How to Set It
Event severity when AppManager failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when AppManager failed to log in	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when HostCPUusage job fails unexpectedly	Set the severity level, from 1 to 40, to indicate the importance of an event in which the HostCPUusage job fails unexpectedly. The default is 5.
Additional Settings	
Event Details	
Event detail format	Select either **HTML Table** or **Plain Text** as the format for event detail. The default is HTML Table.
Monitor CPU Reserved Capacity	
Event Notification	
Raise event when CPU reserved capacity exceeds the threshold?	Select **Yes** to raise an event when CPU reserved capacity exceeds the threshold you set. The default is unselected.
Threshold -- Maximum CPU reserved capacity	Specify the maximum CPU reserved capacity that can occur before an event is raised. The default is 80 percent.
Event severity when CPU reserved capacity exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU reserved capacity exceeds the threshold. The default is 15.
Data Collection	
Collect data for CPU reserved capacity?	Select **Yes** to collect data about CPU reserved capacity for charts and reports. The default is unselected.
Monitor CPU Usage	
Event Notification	
Raise event when CPU usage in MHz exceeds the threshold?	Select **Yes** to raise an event when CPU usage in MHz exceeds the threshold you set. The default is Yes.
Threshold -- Maximum CPU usage in MHz	Specify the maximum CPU usage in MHz that can occur before an event is raised. The default is 2000 MHz.
Event severity when CPU usage in MHz exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage in MHz exceeds the threshold. The default is 15.
Raise event when percent CPU usage exceeds the threshold?	Select **Yes** to raise an event when the percentage of CPU usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum percent CPU usage	Specify the maximum percentage of CPU usage that can occur before an event is raised. The default is 80 percent.
Event severity when percent CPU usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of CPU usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for CPU usage in MHz?	Select **Yes** to collect data about CPU usage in MHz for charts and reports. The default is unselected.
Collect data for average CPU usage as percent?	Select **Yes** to collect data about the average CPU usage as a percentage for charts and reports. The default is unselected.
Collect data for individual CPU usage as percent?	Select **Yes** to collect data about usage for individual CPUs as a percentage for charts and reports. The default is unselected.
Monitor CPU Used	

Parameter	How to Set It
Event Notification	
Raise event when CPU used exceeds the threshold?	Select **Yes** to raise an event when CPU used exceeds the threshold you set. The default is Yes.
Threshold -- Maximum CPU used	Specify the maximum CPU used that can occur before an event is raised. The default is 80 percent.
Event severity when CPU used exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU used exceeds the threshold. The default is 15.
Data Collection	
Collect data for average CPU used?	Select **Yes** to collect data about average CPU used for charts and reports. The default is unselected.
Collect data for individual CPU used?	Select **Yes** to collect data about individual CPU used for charts and reports. The default is unselected.

HostDataStoreUsage

Use this Knowledge Script to monitor host datastore usage. Raises an event when the percentage of available datastore free space falls below the threshold or when the percentage of used datastore free space exceeds the threshold.

Note
When a host goes into maintenance mode all host scripts, except for the HostConnected Knowledge Script, suppress events and data.

Resource Object

vCenter-monitored host. For example, ESX server.

Default Schedule

By default, this script runs every **three hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when available free space falls below the threshold?	Select **Yes** to raise an event if the amount of datastore free space falls below the threshold you set. The default is Yes.
Event severity when available free space falls below the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of available free space falls below the threshold. The default is 15.
Raise event when the percentage of used datastore exceeds the threshold	Select **Yes** to raise an event if the percentage of used datastore exceeds the threshold you set. The default is Yes.
Event severity when percentage of used datastore exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of used datastore exceeds the threshold. The default is 15.
Raise event when datastore metrics are not available?	Select **Yes** to raise an event if datastore metrics are not available. The default is unselected.
Event severity when datastore metrics are not available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which datastore metrics are not available. The default is 15.
Event severity when failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when failed to log in	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when HostDataStoreUsage job fails unexpectedly	Set the severity level, from 1 to 40, to indicate the importance of an event in which the HostDataStoreUsage job fails unexpectedly. The default is 5.
Data Collection	

Parameter	How to Set It
Collect data for free space?	Select **Yes** to collect data about available datastore free space for charts and reports. The default is unselected.
Collect data for percentage used?	Select **Yes** to collect data about the percentage of used datastore for charts and reports. The default is unselected.
Monitoring	
Minimum threshold for available datastore free space (MB)	Specify the minimum amount of datastore free space that must be available to prevent an event from being raised. The default is 500 megabytes.
Maximum threshold for datastore percentage used (%)	Specify the maximum amount of datastore that can be used before an event is raised. The default is 90%.

HostDiskIO

Use this Knowledge Script to monitor disk reads/writes for a host. This script raises an event if the amount of reads/writes in megabytes per second exceeds the threshold you set. This script monitors and collects data for the following performance metrics:

- Disk read rate - Rate at which data is read from each LUN (logical unit number) on the host.
- Disk write rate - Rate at which data is written to each LUN (logical unit number) on the host.

If this script is running in addition to the CPU usage, Memory usage, or Network I/O scripts, you should instead run the HostCPUUsage, HostMemoryUsage, HostDiskIO, and HostNetworkIO Knowledge Scripts to optimize the resource usage on the vCenter host.

This script generates a pair of data streams for each disk that is configured on a host.

Note
When a host goes into maintenance mode all host scripts, except for the HostConnected Knowledge Script, suppress events and data.

Resource Object

vCenter-monitored host. For example, ESX server.

Default Schedule

By default, this script runs every **15 minutes**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when total disk IO exceeds the threshold?	Select **Yes** to raise an event when total disk IO exceeds the threshold you set. The default is unselected.
Event severity when total disk IO exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which total disk IO exceeds the threshold. The default is 15.
Raise event when disk reads exceed the threshold?	Select **Yes** to raise an event if the amount of disk reads exceeds the threshold you set. The default is Yes.
Event severity when disk reads exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of disk reads exceeds the threshold. The default is 15.
Raise event when disk writes exceed the threshold?	Select **Yes** to raise an event if the amount of disk writes exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Event severity when disk writes exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of disk writes exceeds the threshold. The default is 15.
Raise event host is either disconnected or removed?	Select **Yes** to raise an event if the host is either disconnected or removed. The default is Yes.
Event severity when host is either disconnected or removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the host is either disconnected or removed. The default is 15.
Event severity when failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when HostDiskIO job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HostDiskIO job fails unexpectedly. The default is 5.
Data Collection	
Collect data for total disk IO?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the amount of total disk IO. The default is unselected.
Collect data for disk reads?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the amount of disk reads. The default is unselected.
Collect data for individual disk reads?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the amount of individual disk reads. The default is unselected.
Collect data for disk writes?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the amount of disk writes in megabytes per second. The default is unselected.
Collect data for individual disk writes?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the amount of individual disk writes in megabytes per second. The default is unselected.
Monitoring	
Maximum threshold for total disk IO (MBytes/sec)	Specify the maximum amount of total disk IO that can occur before an event is raised. The default is 20 megabytes per second.
Maximum threshold for disk reads (MBytes/sec)	Specify the maximum amount of disk reads that can occur before an event is raised. The default is 2 megabytes per second.
Maximum threshold for disk writes (MBytes/sec)	Specify the maximum amount of disk writes that can occur before an event is raised. The default is 2 megabytes per second.

HostDiskTotalLatency

Use this Knowledge Script to track statistics for disk input/output (I/O) performance metrics for the host. This script monitors and collects data for the following disk latency performance metrics:

- Disk command latency - Average amount of time taken during the collection interval to process a SCSI (Small Computer System Interface) command.
- Disk read latency - Average amount of time taken during the collection interval to process a SCSI read command.
- Disk write latency - Average amount of time taken during the collection interval to process a SCSI write command.
- Commands - Number of SCSI commands issued during the collection interval.
- Aborted commands - Number of SCSI commands aborted during the collection interval.
- Bus resets - Number of SCSI bus reset commands issued during the collection interval.

Notes

- When a host goes into maintenance mode all host scripts, except for the HostConnected Knowledge Script, suppress events and data.
- If you do any of the following, rescan the host bus adapters (HBAs) to ensure the vCenter inventory is up-to-date:

  - Make changes to storage disks or logical unit numbers (LUNs) available to your ESX/ESXi system
  - Make changes to storage adapters
  - Create a new datastore or remove an existing one
  - Reconfigure an existing datastore, for example when you add a new extent

  After completing the rescan, restart the HostDiskTotalLatency job or wait 24 hours for it to repopulate its storage adapter cache.

Resource Object

vCenter-monitored host. For example, ESX server.

Default Schedule

By default, this script runs **Every 15 minutes**.

Note

If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event when latency metrics are not available?	Select **Yes** to raise an event when latency metrics are not available. The default is unselected.
Event severity when latency metrics are not available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which latency metrics are not available. The default is 15.
Raise event when host is either disconnected or removed?	Select **Yes** to raise an event when the host is either disconnected or removed. The default is Yes.
Event severity when host is either disconnected or removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the host is either disconnected of removed. The default is 15.
Event severity when AppManager failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to get metrics. The default is 15.
Event severity when AppManager failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in. The default is 5.
Event severity when HostDiskTotalLatency job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HostDiskTotalLatency job fails unexpectedly. The default is 5.
Additional Settings	
Event Details	
Event detail format	Select either **HTML Table** or **Plain Text** as the format for event detail. The default is HTML Table.
Monitor Disk Latency	
Event Notification	
Raise event if disk command latency exceeds the threshold?	Select **Yes** to raise an event if disk command latency exceeds the threshold you set. The default is Yes.
Threshold -- Maximum disk command latency	Specify the maximum disk command latency that can occur before an event is raised. The default is 10 milliseconds.
Event severity when disk command latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which disk command latency exceeds the threshold. The default is 15.
Raise event if disk read latency exceeds the threshold?	Select **Yes** to raise an event if disk read latency exceeds the threshold you set. The default is Yes.
Threshold -- Maximum disk read latency	Specify the maximum disk read latency that can occur before an event is raised. The default is 10 milliseconds.
Event severity when disk read latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which disk read latency exceeds the threshold. The default is 15.
Raise event if disk write latency exceeds the threshold?	Select **Yes** to raise an event if disk write latency exceeds the threshold you set. The default is Yes.
Threshold -- Maximum disk write latency	Specify the maximum disk write latency that can occur before an event is raised. The default is 10 milliseconds.

Parameter	How to Set It
Event severity when disk write latency exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which disk write latency exceeds the threshold. The default is 15.
Data Collection	
Collect data for disk command latency?	Select **Yes** to collect disk command latency data for charts and reports. The default is unselected.
Collect data for disk read latency?	Select **Yes** to collect disk read latency data for charts and reports. The default is unselected.
Collect data for disk write latency?	Select **Yes** to collect disk write latency data for charts and reports. The default is unselected.
Monitor Commands	
Event Notification	
Raise event if commands exceeds the threshold?	Select **Yes** to raise an event if the number of SCSI commands issued during the collection interval exceeds the threshold you set. The default is unselected.
Threshold -- Maximum commands	Specify the maximum number of SCSI commands that can occur before an event is raised. The default is 15000.
Event severity when commands exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of SCSI commands exceeds the threshold. The default is 15.
Raise event if aborted commands exceeds the threshold?	Select **Yes** to raise an event if the number SCSI commands aborted during the collection interval exceeds the threshold you set. The default is unselected.
Threshold -- Maximum aborted commands	Specify the maximum number of SCSI commands that can be aborted before an event is raised. The default is 10.
Event severity if aborted commands exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of aborted SCSI commands exceeds the threshold. The default is 15.
Data Collection	
Collect data for commands?	Select **Yes** to collect commands data for charts and reports. The default is unselected.
Collect data for aborted commands?	Select **Yes** to collect aborted commands data for charts and reports. The default is unselected.
Monitor Bus Resets	
Event Notification	
Raise event if bus resets exceeds the threshold?	Select **Yes** to raise an event if the number of bus resets exceeds the threshold you set. The default is unselected.
Threshold -- Maximum bus resets	Specify the maximum number of bus resets that can occur before an event is raised. The default is 10.
Event severity when bus resets exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which bus resets exceed the threshold. The default is 15.
Data Collection	
Collect data for bus resets?	Select **Yes** to collect data for bus resets for charts and reports. The default is unselected.

HostMemoryUsage

Use this Knowledge Script to monitor the following memory metrics for a host:

- Memory active - Sum of active memory for all powered-on virtual machines plus vSphere services (such as COS, vpxa) on the host.
- Memory balloon - Sum of memory balloon of all powered-on virtual machines and vSphere services on the host. If the balloon target value is greater than the balloon value, the VMkernel inflates the balloon, causing more virtual machine memory to be reclaimed. If the balloon target value is less than the balloon value, the VMkernel deflates the balloon, which allows the virtual machine to consume additional memory if needed.
- Memory granted - Sum of granted memory for all powered-on virtual machines, plus machine memory for vSphere services on the host.
- Memory overhead - Total of all overhead memory for powered-on virtual machines, plus the overhead of running vSphere services on the host.
- Memory reserved - Amount of memory (in kilobytes) that has been reserved, in particular for resource pools and virtual machines.
- Memory shared - Sum of shared memory for all powered-on virtual machines, plus amount for vSphere services on the host. The host's shared memory may be larger than the amount of machine memory if memory is overcommitted (the aggregate virtual machine configured memory is much greater than machine memory). The value of this statistic reflects how effective transparent page sharing and memory over-commitment are for saving machine memory.
- Memory shared common - Amount of machine memory that is shared by all powered-on virtual machines and vSphere services on the host. Subtract this metric from the shared metric to gauge how much machine memory is saved due to sharing.
- Memory state - Amount of free machine memory on the host. The VMkernel has four free-memory thresholds that affect memory reclamation:
  - 0 (high) Free memory ≥ 6% of machine memory minus Service Console memory.
  - 1 (soft) 4%
  - 2 (hard) 2%
  - 3 (low) 1%
  - 0 (high) and 1 (soft): Swapping is favored over ballooning
  - 2 (hard) and 3 (low): Ballooning is favored over swapping
- Memory swap in - Sum of swap in values for all powered-on virtual machines on the host.
- Memory swap in rate - Rate at which memory is swapped from disk into active memory.
- Memory swap out - Sum of swap out memory from all powered-on virtual machines on the host.
- Memory swap out rate - Rate at which memory is being swapped from active memory to disk during the current interval. This counter applies to virtual machines and is generally more useful than the swap out counter to determine if the virtual machine is running slow due to swapping, especially when looking at real-time statistics.
- Memory swap used - Sum of the memory swapped by all powered-on virtual machines on the host.
- Memory unreserved - Amount of memory that is unreserved. Memory reservation not used by the Service Console, VMkernel, vSphere services and other powered-on virtual machines user-specified memory reservations and overhead memory. This statistic is no longer relevant to virtual machine admission control, as reservations are now handled through resource pools.

- Memory usage - Percentage of available machine memory usage:
- Memory zero - Sum of zero memory for all powered-on virtual machines, plus vSphere services on the host.

This script raises an event if a monitored metric exceeds the threshold you set.

If this script is running in addition to the Disk I/O, CPU usage, or Network I/O scripts, you should instead run the HostCPUUsage, ClusterMemUsage, HostDiskIO, and HostNetworkIO Knowledge Scripts to optimize the resource usage on the vCenter host.

Note
When a host goes into maintenance mode all host scripts, except for the HostConnected Knowledge Script, suppress events and data.

Resource Object

vCenter-monitored host. For example, ESX server.

Default Schedule

By default, this script runs every **15 minutes**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event when host is either disconnected or removed?	Select **Yes** to raise an event when the host is either disconnected or removed. The default is Yes.
Event severity when host is either disconnected or removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in the host is either disconnected or removed. The default is 15.
Raise event when memory metrics are not available?	Select **Yes** to raise an event when memory metrics are not available. The default is Yes.
Event severity when memory metrics are not available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory metrics are not available. The default is 15.
Event severity when AppManager failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when AppManager failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.

Parameter	How to Set It
Event severity when HostMemoryUsage job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HostMemoryUsage job fails unexpectedly. The default is 5.
Additional Settings	
Event Details	
Event detail format	Select either **HTML Table** or **Plain Text** as the format for event detail. The default is HTML Table.
Monitor Memory Active	
Event Notification	
Raise event when memory active exceeds the threshold?	Select **Yes** to raise an event when the memory active exceeds the threshold you set. The default is unselected.
Threshold -- Maximum memory active	Specify the maximum threshold for memory active that can be reached before an event is raised. The default is 20 percent.
Event severity when memory active exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event when the active memory exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory active?	Select **Yes** to collect data about memory active for charts and reports. The default is unselected.
Monitoring Memory Balloon	
Event Notification	
Raise an event when memory balloon exceeds the threshold?	Select **Yes** to raise an event when host memory balloon exceeds the threshold you set. The default is Yes.
Threshold -- Maximum memory balloon	Specify the maximum threshold for memory balloon that can be reached before an event is raised. The default is 2 percent.
Event severity when memory balloon exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which host memory balloon exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory balloon?	Select **Yes** to collect data about host memory balloon for charts and reports. The default is unselected.
Monitor Memory Granted	
Event Notification	
Raise event when memory granted exceeds the threshold?	Select **Yes** to raise an event when the amount of memory granted exceeds the threshold you set. The default is unselected.
Threshold -- Maximum memory granted	Specify the maximum threshold for memory granted that can be reached before an event is raised. The default is 80 percent.
Event severity when memory granted exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of memory granted exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory granted?	Select **Yes** to collect data about memory granted for charts and reports. The default is unselected.
Monitor Memory Overhead	
Event Notification	
Raise event when memory overhead exceeds the threshold?	Select **Yes** to raise an event when the amount of memory overhead exceeds the threshold you set. The default is unselected.

Parameter	How to Set It
Threshold -- Maximum for memory overhead	Specify the maximum threshold for memory overhead that can be reached before an event is raised. The default is 512 megabyte.
Event severity when memory overhead exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of memory overhead exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory overhead?	Select **Yes** to collect data about memory overhead for charts and reports. The default is unselected.
Memory Reserved Capacity	
Event Notification	
Raise event when memory reserved capacity exceeds the threshold?	Select **Yes** to raise an event when memory reserved capacity exceeds the threshold you set. The default is unselected.
Threshold -- Maximum for memory reserved capacity	Specify the maximum threshold for memory reserved capacity that can be reached before an event is raised. The default is 80 percent.
Event severity when memory reserved capacity exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which host memory reserved capacity exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory reserved capacity?	Select **Yes** to collect data about memory reserved capacity for charts and reports. The default is unselected.
Monitor Memory Shared	
Event Notification	
Raise event when memory shared falls below the threshold?	Select **Yes** to raise an event when memory shared falls below the threshold you set. The default is unselected.
Threshold -- Minimum for memory shared	Specify the minimum threshold for memory shared that can be reached before an event is raised. The default is 512 megabytes.
Event severity when memory shared falls below the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory shared falls below the threshold. The default is 15.
Data Collection	
Collect data for memory shared?	Select **Yes** to collect data about memory shared for charts and reports. The default is unselected.
Monitor Memory Shared Common	
Event Notification	
Raise event when memory shared common falls below the threshold?	Select **Yes** to raise an event when memory shared common falls below the threshold you set. The default is unselected.
Threshold -- Minimum for memory shared common	Specify the minimum threshold for memory shared common that can be reached before an event is raised. The default is 256 megabytes.
Event severity when memory shared common falls below the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory shared common falls below the threshold. The default is 15.
Data Collection	
Collect data for memory shared common?	Select **Yes** to collect data about memory shared common for charts and reports. The default is unselected.
Monitor Memory State	
Event Notification	
Raise event when memory state is hard?	Select **Yes** to raise an event when memory state is hard. The default is unselected.

Parameter	How to Set It
Event severity when memory state is hard	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the memory state is hard. The default is 10.
Raise event when memory state is high?	Select **Yes** to raise an event when memory state is high. The default is unselected.
Event severity when memory state is high	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the memory state is high. The default is 25.
Raise event when memory state is low?	Select **Yes** to raise an event when memory state is low. The default is unselected.
Event severity when memory state is low	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the memory state is low. The default is 5.
Raise event when memory state is soft?	Select **Yes** to raise an event when memory state is soft. The default is unselected.
Event severity when memory state is soft	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the memory state is soft. The default is 15.
Data Collection	
Collect data for memory state?	Select **Yes** to collect data about memory state for charts and reports. The default is unselected.
Monitor Memory Swap In	
Event Notification	
Raise event when memory swap in exceeds the threshold?	Select **Yes** to raise an event when memory swap in exceeds the threshold you set. The default is unselected.
Threshold -- Maximum for memory swap in rate	Specify the maximum threshold for memory swap in rate that can be reached before an event is raised. The default is 512 megabytes.
Event severity when memory swap in exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which host memory swap in exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory swap in?	Select **Yes** to collect data about memory swap in for charts and reports. The default is unselected.
Monitor Memory Swap In Rate	
Event Notification	
Raise event when memory swap in rate exceeds the threshold?	Select **Yes** to raise an event when memory swap rate in exceeds the threshold you set. The default is Yes.
Threshold -- Maximum for memory swap in rate	Specify the maximum threshold for memory swap in rate that can be reached before an event is raised. The default is 1 megabyte per second .
Event severity when memory swap in rate exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which host memory swap in rate exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory swap in rate?	Select **Yes** to collect data about memory swap in rate for charts and reports. The default is unselected.
Monitor Memory Swap Out	
Event Notification	
Raise event when memory swap out exceeds the threshold?	Select **Yes** to raise an event when memory swap out exceeds the threshold you set. The default is unselected.
Threshold -- Maximum for memory swap out	Specify the maximum threshold for memory swap out that can be reached before an event is raised. The default is 256 megabytes.

Parameter	How to Set It
Event severity when memory swap out exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which host memory swap out exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory swap out?	Select **Yes** to collect data about memory swap out for charts and reports. The default is unselected.
Monitor Memory Swap Out Rate	
Event Notification	
Raise event when memory swap out rate exceeds the threshold?	Select **Yes** to raise an event when memory swap out rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum for memory swap out rate	Specify the maximum threshold for memory swap out rate that can be reached before an event is raised. The default is 1 megabyte per second.
Event severity when memory swap out rate exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory swap out rate exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory swap out rate?	Select **Yes** to collect data about memory swap out rate for charts and reports. The default is unselected.
Monitor Memory Swap Used	
Event Notification	
Raise event when memory swap used exceeds the threshold?	Select **Yes** to raise an event when memory swap used exceeds the threshold you set. The default is Yes.
Threshold -- Maximum for memory swap used	Specify the maximum threshold for memory swap used that can be reached before an event is raised. The default is 2.
Event severity when memory swap used exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory swap used exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory swap used?	Select **Yes** to collect data about memory swap used for charts and reports. The default is unselected.
Monitor Memory Unreserved	
Event Notification	
Raise event when memory unreserved exceeds the threshold?	Select **Yes** to raise an event when memory unreserved exceeds the threshold you set. The default is unselected.
Threshold -- Maximum for memory unreserved	Specify the maximum threshold for memory unreserved that can be reached before an event is raised. The default is 80 percent.
Event severity when memory unreserved exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which host memory unreserved exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory unreserved?	Select **Yes** to collect data about memory unreserved for charts and reports. The default is unselected.
Monitor Memory Usage	
Event Notification	
Raise event when memory usage exceeds the threshold?	Select **Yes** to raise an event when memory usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum for memory usage	Specify the maximum threshold for memory usage that can be reached before an event is raised. The default is 80 percent.

Parameter	How to Set It
Event severity when memory usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which host memory usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory usage?	Select **Yes** to collect data about memory usage for charts and reports. The default is unselected.
Monitor Memory Usage by VMKernel	
Event Notification	
Raise event when memory usage by VMkernel exceeds the threshold?	Select **Yes** to raise an event when memory usage by VMkernel exceeds the threshold you set. The default is unselected.
Threshold -- Maximum for memory usage by VMkernel	Specify the maximum threshold for memory usage by VMkernel that can be reached before an event is raised. The default is 256 megabytes.
Event severity when memory usage by VMkernel exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory usage by VMkernel exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory usage by VMkernel?	Select **Yes** to collect data about memory usage for VMkernel for charts and reports. The default is unselected.
Monitor Memory Zero	
Event Notification	
Raise event when memory zero exceeds the threshold?	Select **Yes** to raise an event when memory zero exceeds the threshold you set. The default is unselected.
Threshold - Maximum for memory zero	Specify the maximum threshold for memory zero that can be reached before an event is raised. The default is 20 percent.
Event severity when memory zero exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory zero exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory zero?	Select **Yes** to collect data about memory zero for charts and reports. The default is unselected.

HostNetworkIO

Use this Knowledge Script to monitor network reads/writes for a vCenter host. This script raises an event if the rate of network reads/writes exceeds the threshold you set.

- Network reads - The rate at which data is received across each physical NIC instance on the host.
- Network writes - The rate at which data is written to each LUN (logical unit number) on the host.

Note
When a host goes into maintenance mode, all host scripts, except for the HostConnected Knowledge Script, suppress events and data.

Resource Object

vCenter-monitored host. For example, ESX server

Default Schedule

By default, this script runs every **15 minutes**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when network reads exceed the threshold?	Select **Yes** to raise an event if the rate of network reads exceeds the threshold you set. The default is Yes.
Event severity when network reads exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the rate of network reads exceeds the threshold. The default is 15.
Raise event when individual network reads exceed the threshold?	Select **Yes** to raise an event if the rate of individual network reads exceeds the threshold you set. The default is unselected.
Event severity when individual network reads exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the rate of individual network reads exceeds the threshold. The default is 15.
Raise event when network writes exceed the threshold?	Select **Yes** to raise an event if the rate of network writes exceeds the threshold you set. The default is Yes.
Event severity when network writes exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the rate of individual network writes exceeds the threshold. The default is 15.
Raise event when individual network writes exceed the threshold?	Select **Yes** to raise an event if the rate of individual network writes exceeds the threshold you set. The default is unselected.

Parameter	How to Set It
Event severity when individual network writes exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the rate of individual network writes exceeds the threshold. The default is 15.
Raise event when host is either disconnected or removed?	Select **Yes** to raise an event if the host is either disconnected or removed. The default is Yes.
Event severity when host is either disconnected or removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the host is either disconnected or removed. The default is 15.
Event severity when AppManager failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when AppManager failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when HostNetworkIO job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HostNetworkIO job fails unexpectedly. The default is 5.
Data Collection	
Collect data for network reads?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate of network reads in megabytes per second. The default is unselected.
Collect data for individual network reads?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate of individual network reads in megabytes per second. The default is unselected.
Collect data for network writes?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate of network writes in megabytes per second. The default is unselected.
Collect data for individual network writes?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the rate of individual network writes in megabytes per second. The default is unselected.
Monitoring	
Maximum threshold for network reads	Specify the maximum rate of network reads that can occur before an event is raised. The default is 2 megabytes per second.
Maximum threshold for individual network reads	Specify the maximum rate of individual network reads that can occur before an event is raised. The default is 2 megabytes per second.
Maximum threshold for network writes	Specify the maximum rate of network writes that can occur before an event is raised. The default is 2 megabytes per second.
Maximum threshold for individual network writes	Specify the maximum rate of individual network writes that can occur before an event is raised. The default is 2 megabytes per second.

HWCorrectableMemCondition

Use this Knowledge Script to monitor the state of correctable memory devices. This script uses SNMP to gather the correctable memory condition information.

The text of an event message indicates the state:

- **Failed**, when the correctable memory device is not operating properly.
- **Degraded**, when the memory module's correctable error count has exceeded the threshold.
- **Other**, when the status is unknown or could not be determined.

Prerequisites

- Configure AppManager Security Manager with the information that provides SNMP access to vCenter hosts.
- Run the ConfigureHostTraffic Knowledge script to enable an SNMP firewall port for a given host.
- This script queries the SNMP agent on individual ESX servers and does not depend on vCenter services. If an SNMP port is not enabled by the firewall, run ConfigureHostTraffic to enable a port.

Resource Objects

vCenter host objects

Default Schedule

By default, this script runs every **15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event if hardware not responding?	Select **Yes** to raise an event if correctable memory devices are not responding. The default is Yes.
Event severity when hardware is not responding	Set the event severity level, from 1 to 40, to indicate the importance of an event in which correctable memory devices are not responding. The default is 15.
Raise event if hardware is not supported?	Select **Yes** to raise an event if correctable memory devices are not supported, for example do not have SNMP installed, the host is not HP or Dell hardware, or ports are not enabled. The default is Yes.
Event severity when hardware is not supported	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a correctable memory devices are not supported. The default is 15.
Event severity when HWCorrectableMemCondition job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HWCorrectableMemCondition job fails unexpectedly. The default is 5.
SNMP Settings	

Parameter	How to Set It
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Monitor Correctable Memory Device Status	
Event Notification	
Raise event if device status is "Ok?"	Select **Yes** to raise an event if the status of a correctable memory device is "Ok". The default is unselected.
Event severity when device status is "Ok"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a correctable memory device is "Ok". The default is 25.
Raise event if device status is "Degraded?"	Select **Yes** to raise an event if status of a correctable memory device is "Degraded". The default is Yes.
Event severity when device status is "Degraded"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a correctable memory device is "Degraded". The default is 15.
Raise event if device status is "Failed" or Critical?"	Select **Yes** to raise an event if the status of a correctable memory device is "Failed" or "Critical". The default is Yes.
Event severity when device status is "Failed" or "Critical"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a correctable memory device is "Failed" or "Critical". The default is 10.
Raise event if device status is "Unknown?"	Select **Yes** to raise an event if the status of a correctable memory device is "Unknown". The default is Yes.
Event severity when device status is "Unknown"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a correctable memory device is "Unknown". The default is 15.
Raise event if device status is "Other?"	Select **Yes** to raise an event if the status of a correctable memory device is "Other". The default is Yes.
Event severity when device status is "Other"	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a correctable memory device is "Other". The default is 15.
Data Collection	
Collect data for device status?	Select **Yes** to collect data for graphs and reports. When enabled, returns a data stream for each SNMP device/SNMP attribute pair. The default is Yes.

HWFanStatus(CPU)

Use this Knowledge Script to monitor the state of the CPU fan. This Knowledge Script uses SNMP to find the CPU fan attached to the agent.

This Knowledge Script runs on HP Insight Manager resources only.

The text of an event message indicates the state:

- **Failed**, when the fan is not operating properly.
- **Other**, when the system or driver does not support the fan status detection.

Prerequisites

- Configure AppManager Security Manager with the information that provides SNMP access to vCenter hosts.
- This script queries the SNMP agent on individual ESX servers and does not depend on vCenter services. If an SNMP port is not enabled by the firewall, run ConfigureHostTraffic to enable a port.

Resource Objects

vCenter host objects

Default Schedule

By default, this script runs every **15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event if hardware not responding?	Select **Yes** to raise an event if CPU fans are not responding. The default is Yes.
Event severity when hardware is not responding	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU fans are not responding. The default is 15.
Raise event if hardware is not supported?	Select **Yes** to raise an event if CPU fans are not supported, for example do not have SNMP installed, the host is not HP or Dell hardware, or ports are not enabled. The default is Yes.
Event severity when hardware is not supported	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU fans are not supported. The default is 15.
Event severity when HWFanStatus(CPU) job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HWFanStatus(CPU) job fails unexpectedly. The default is 5.
SNMP Settings	
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.

Parameter	How to Set It
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Monitor Fan Status	
Event Notification	
Raise event if fan status is "Ok?"	Select **Yes** to raise an event if the status of a CPU fan is "Ok". The default is unselected.
Event severity when fan status is "Ok"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a CPU fan is "Ok". The default is 25.
Raise event if fan status is "Failed?"	Select **Yes** to raise an event if the status of a CPU fan is "Failed". The default is Yes.
Event severity when fan status is "Failed"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a CPU fan is "Failed" default is 10.
Raise event if fan status is "Unknown?"	Select **Yes** to raise an event if the status of a system fan is "Unknown". The default is Yes.
Event severity when fan status is "Unknown"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a system fan is "Unknown". The default is 15.
Raise event if fan status is "Other?"	Select **Yes** to raise an event if the status of a CPU fan is "Other". The default is Yes.
Event severity when fan status is "Other"	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a CPU fan is "Other". The default is 15.
Data Collection	
Collect data for fan status?	Select **Yes** to collect data for graphs and reports. When enabled, returns a data stream for each SNMP device/SNMP attribute pair. The default is Yes.

HWFanStatus(System)

Use this Knowledge Script to monitor the state of the system fan. This script uses the UDP port number to find the system fan attached to the agent and monitors its state.

The text of an event message indicates the state:

- **Failed**, when a required fan is not operating properly.
- **Degraded**, when a non-required fan is not operating properly.
- **Other**, when this system or driver does not support the fan status detection.

Prerequisites

- Configure AppManager Security Manager with the information that provides SNMP access to vCenter hosts.
- This script queries the SNMP agent on individual ESX servers and does not depend on vCenter services. If an SNMP port is not enabled by the firewall, run ConfigureHostTraffic to enable a port.

Resource Objects

vCenter host objects

Default Schedule

By default, this script runs every **15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event if hardware not responding?	Select **Yes** to raise an event if system fans are not responding. The default is Yes.
Event severity when hardware is not responding	Set the event severity level, from 1 to 40, to indicate the importance of an event in which system fans are not responding. The default is 15.
Raise event if hardware is not supported?	Select **Yes** to raise an event if system fans are not supported, for example do not have SNMP installed, the host is not HP or Dell hardware, or ports are not enabled. The default is Yes.
Event severity when hardware is not supported	Set the event severity level, from 1 to 40, to indicate the importance of an event in which system fans are not supported. The default is 15.
Event severity when HWFanStatus(System) job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HWFanStatus(System) job fails unexpectedly. The default is 5.
SNMP Settings	
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.

Parameter	How to Set It
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Monitor System Fan Status	
Event Notification	
Raise event if fan status is "Ok?"	Select **Yes** to raise an event if the status of a system fan is "Ok". The default is unselected.
Event severity when fan status is "Ok"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a system fan is "Ok". The default is 25.
Raise event if fan status is "Degraded?"	Select **Yes** to raise an event if status of system fan is "Degraded". The default is Yes.
Event severity when fan status is "Degraded"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a system fan is "Degraded". The default is 15.
Raise event if fan status is "Failed?"	Select **Yes** to raise an event if the status of a system fan is "Failed". The default is Yes.
Event severity when fan status is "Failed"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a system fan is "Failed". The default is 10.
Raise event if fan status is "Unknown?"	Select **Yes** to raise an event if the status of a system fan is "Unknown". The default is Yes.
Event severity when fan status is "Unknown"	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a system fan is "Unknown". The default is 15.
Raise event if fan status is "Other?"	Select **Yes** to raise an event if the status of a system fan is "Other". The default is Yes.
Event severity when fan status is "Other"	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a system fan is "Other". The default is 15.
Data Collection	
Collect data for fan status?	Select **Yes** to collect data for graphs and reports. When enabled, returns a data stream for each SNMP device/SNMP attribute pair. The default is Yes.

HWHPNICLost

Use this Knowledge Script to monitor the AppManager for VMware managed client computer for incoming SNMPv1 trap messages as they are received.

This Knowledge Script runs on HP Insight Manager resources only.

This script monitors HP ESX hosts, using specific object identifiers: 18002 or 18006. This script monitors for any time the status of a logical adapter changes to the Failed condition. A Failed condition occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. Failure can be caused by loss of link because of a cable being removed. Internal adapter, hub, or switch failures can also cause this condition.

To enable this script to work properly, do **not** enable event collapsing in the **Advanced** tab of the job's Properties dialog box.

Use this script in conjunction with the HWHPNICRestorScripted Knowledge Script to monitor the logical adapter status on your HP ESX hosts. To report on the number of times that a logical adapter was down, configure this script to collect data. By default, this script does not collect data.

You can specify search criteria to filter for trap messages from SNMP-enabled applications and devices. This script raises an event when a trap message matches all of the search criteria. All trap messages that match the filtering criteria are returned in the event.

This script requires the Microsoft **SNMP Trap** service to be running on the managed client computer.

This script monitors only new trap messages received by the managed client computer.

Resource Objects

vCenter servers

Default Schedule

The default interval for this script is **Asynchronous**. Regardless of the schedule you select, once you start the Knowledge Script, its job status appears as **Running**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event?	Select **Yes** to raise an event when a trap message matches all of the search criteria. The event message contains all trap messages that match the filtering criteria. The default is Yes.
Collect data?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns data about Failed status conditions. The default is No.

Parameter	How to Set It
Filter by IP source address	Identify the trap message source you want to filter by specifying the Internet Protocol (IP) address of the SNMP source. Specify the IP address using “dot” notation. For example: `10.10.10.10` To filter trap messages from more than one IP address, separate each address with a comma, without any spaces. If you leave this parameter blank, the script does not use the IP address of the SNMP agent that sent the trap message to filter for events. The filter string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter by generic trap number	Provide a generic trap number to filter trap messages that use the same object identifier (OID) for more than one trap message. You usually do not need to filter for generic and specific trap message numbers if the OID is unique. If you leave this parameter blank, the script does not use a generic value to filter for events. The generic value of the OID is defined by the SNMP source agent. The filter string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which trap messages match your search criteria. The default is 5. You can adjust the severity depending on which type of message you are checking for.

HWHPNICRestorScripted

Use this Knowledge Script to monitor the AppManager for VMware managed client computer for incoming SNMPv1 trap messages as they are received.

This Knowledge Script runs on HP Insight Manager resources only.

This Knowledge Script monitors HP ESX hosts, using specific object identifiers: 18001 or 18005. This trap will be sent any time connectivity is restored to a logical adapter. The connectivity to a logical adapter occurs in one of the following conditions:

- When the physical adapter in a single adapter configuration returns to the OK condition
- When at least one physical adapter in a logical adapter group returns to the OK condition

Connectivity can be restored by the replacement of a faulty cable or by re-attaching a cable that was unplugged.

To enable this script to work properly, do **not** enable event collapsing in the **Advanced** tab of the job's Properties dialog box.

Use this script in conjunction with the HWHPNICLost Knowledge Script to monitor the logical adapter status on your HP ESX hosts.

You can specify search criteria to filter for trap messages from SNMP-enabled applications and devices. When a trap message matches all of the search criteria, an AppManager for VMware event is raised. All trap messages that match the filtering criteria are returned in the event.

This script requires the Microsoft **SNMP Trap** service is running on the managed client computer.

When you run this script, only new trap messages received by the managed client computer are monitored.

Resource Objects

vCenter servers

Default Schedule

The default interval for this script is **Asynchronous**. Regardless of the schedule you select, once you start the Knowledge Script, its job status appears as **Running**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event?	Select **Yes** to raise an event if trap message matches all of the search criteria. The default is Yes.
Collect data?	Select **Yes** to collect data about connectivity status. By default, data is not collected.

Parameter	How to Set It
Filter by IP source address	Identify the trap message source you want to filter by specifying the Internet Protocol (IP) address of the SNMP source. Specify the IP address using “dot” notation. For example: `10.10.10.10` To filter trap messages from more than one IP address, separate each address with a comma, without any spaces. If you leave this parameter blank, the script does not use the IP address of the SNMP agent that sent the trap message to filter for events. The filter string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter by generic trap number	Provide a generic trap number to filter trap messages that use the same object identifier (OID) for more than one trap message. You usually do not need to filter for generic and specific trap message numbers if the OID is unique. If you leave this parameter blank, the script does not use a generic value to filter for events. The generic value of the OID is defined by the SNMP source agent. The filter string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which trap messages match your search criteria. The default is 5. You may want to adjust the severity depending on which type of message you are checking for.

HWLogicalDiskStatus

Use this Knowledge Script to monitor the state of the logical disk. This script uses the UDP port number to find the logical disk attached to the agent.

The text of an event message indicates the state:

- **Failed**, when more physical drives have failed than the fault tolerance mode of the logical drive can handle without data loss.
- **Other**, when the logical drive is in a state other than normal or failed.

Prerequisites

- Configure AppManager Security Manager with the information that provides SNMP access to vCenter hosts.
- This script queries the SNMP agent on individual ESX servers and does not depend on vCenter services. If an SNMP port is not enabled by the firewall, run ConfigureHostTraffic to enable a port.

Resource Objects

vCenter host objects

Default Schedule

By default, this script runs every **15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event if hardware is not responding?	Select **Yes** to raise an event if logical disks are not responding. The default is Yes.
Event severity when hardware is not responding	Set the event severity level, from 1 to 40, to indicate the importance of an event in which logical disks are not responding. The default is 15.
Raise event if hardware is not supported?	Select **Yes** to raise an event if logical disks are not supported, for example do not have SNMP installed, the host is not HP or Dell hardware, or ports are not enabled. The default is Yes.
Event severity when hardware is not supported	Set the event severity level, from 1 to 40, to indicate the importance of an event in which logical disks are not being supported. The default is 15.
Event severity when HWLogicalDiskStatus job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HWLogicalDiskStatus job fails unexpectedly. The default is 5.
SNMP Settings	
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.

Parameter	How to Set It
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Monitor Logical Disk Status	
Event Notification	
Raise event if logical disk status is “Ok?”	Select **Yes** to raise an event if the status of a logical disk is “Ok”. The default is unselected.
Event severity when logical disk status is “Ok”	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a logical disk is “Ok”. The default is 25.
Raise event if logical disk status is “Degraded?”	Select **Yes** to raise an event if status of a logical disk is “Degraded”. The default is Yes.
Event severity when logical disk status is “Degraded”	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a logical disk is “Degraded”. The default is 15.
Raise event if logical disk status is “Failed” or “Failure?”	Select **Yes** to raise an event if the status of a logical disk is “Failed” or “Failure”. The default is Yes.
Event severity when logical disk status is “Failed or “Failure”	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a logical disk is “Failed” or “Failure”. The default is 10.
Raise event if logical disk status is “Offline?”	Select **Yes** to raise an event if the status of a logical disk is “Offline”. The default is Yes.
Event severity when logical disk status is “Offline”	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a logical disk is “Offline”. The default is 15.
Raise event if logical disk status is “Other?”	Select **Yes** to raise an event if the status of a logical disk is “Other”. The default is Yes.
Event severity when logical disk status is “Other”	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a logical disk is “Other”. The default is 15.
Data Collection	
Collect data for disk status?	Select **Yes** to collect data for graphs and reports. When enabled, returns a data stream for each SNMP device/SNMP attribute pair. The default is Yes.

HWPhysicalDiskStatus

Use this Knowledge Script to monitor the state of the physical disk. This script uses the UDP port number to find the logical disk attached to the agent.

The text of an event message indicates the state:

- **Failed**, when the drive is in one of the following conditions that requires drive replacement.
  - The drive no longer operating
  - The drive has a predictive failure error
- **Other**, when the instrument agent does not recognize the drive. You may need to upgrade your instrument agent and driver software.

Before running this script, configure AppManager

Prerequisites

- Configure AppManager Security Manager with the information that provides SNMP access to vCenter hosts.
- This script queries the SNMP agent on individual ESX servers and does not depend on vCenter services. If an SNMP is not enabled by the firewall, run ConfigureHostTraffic to enable a port.

Resource Objects

vCenter host objects

Default Schedule

By default, this script runs every **15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event if hardware is not responding?	Select **Yes** to raise an event if physical disks are not responding. The default is Yes.
Event severity when hardware is not responding	Set the event severity level, from 1 to 40, to indicate the importance of an event in which physical disks are not responding. The default is 15.
Raise event if hardware is not supported?	Select **Yes** to raise an event if physical disks are not supported, for example do not have SNMP installed, the host is not HP or Dell hardware, or ports are not enabled. The default is Yes.
Event severity when hardware is not supported	Set the event severity level, from 1 to 40, to indicate the importance of an event in which physical disks are not being supported. The default is 15.
Event severity when HWPhysicalDiskStatus job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HWPhysicalDiskStatus job fails unexpectedly. The default is 5.
SNMP Settings	

Parameter	How to Set It
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Monitor Physical Disk Status	
Event Notification	
Raise event if disk status is "Ok" or "Operational?"	Select **Yes** to raise an event if the status of a physical disk is "Ok" or "Operational". The default is unselected.
Event severity when disk status is "Ok" or "Operational"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a physical disk is "Ok" or "Operational". The default is 25.
Raise event if disk status is "Degraded?"	Select **Yes** to raise an event if status of a physical disk is "Degraded". The default is Yes.
Event severity when disk status is "Degraded"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a physical disk is "Degraded". The default is 15.
Raise event if disk status is "Failed" or "Failure?"	Select **Yes** to raise an event if the status of a physical disk is "Failed" or "Failure". The default is Yes.
Event severity when disk status is "Failed or "Failure"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a physical disk is "Failed" or "Failure". The default is 10.
Raise event if disk status is "Offline?"	Select **Yes** to raise an event if the status of a physical disk is "Offline". The default is Yes.
Event severity when disk status is "Offline"	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a physical disk is "Offline". The default is 15.
Raise event if disk status is "Recovering?"	Select **Yes** to raise an event if the status of a physical disk is "Recovering". The default is Yes.
Event severity when disk status is "Recovering"	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a physical disk is "Recovering". The default is 15.
Raise event if disk status is "Removed?"	Select **Yes** to raise an event if the status of a physical disk is "Removed". The default is Yes.
Event severity when disk status is "Removed"	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a physical disk is "Removed". The default is 15.
Raise event if disk status is "Other?"	Select **Yes** to raise an event if the status of a physical disk is "Other". The default is Yes.
Event severity when disk status is "Other"	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a physical disk is "Other". The default is 15.
Data Collection	
Collect data for disk status?	Select **Yes** to collect data for graphs and reports. When enabled, returns a data stream for each SNMP device/SNMP attribute pair. The default is Yes.

HWPowerSupply

Use this Knowledge Script to monitor the state of the power supply devices in the system. This script uses the UDP port number to find the power supply device attached to the agent.

The text of an event message indicates the state:

- **Failed**, when a power supply component detects a condition that could permanently damage the system.
- **Degraded**, when a temperature sensor, fan or other power supply component is outside normal operating range.
- **Other**, when the status cannot be determined or is not present.

Prerequisites

- Configure AppManager Security Manager with the information that provides SNMP access to vCenter hosts.
- This script queries the SNMP agent on individual ESX servers and does not depend on vCenter services. If an SNMP port is not enabled by the firewall, run ConfigureHostTraffic to enable a port.

Resource Objects

vCenter host objects.

Default Schedule

By default, this script runs every **15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event if hardware is not responding?	Select **Yes** to raise an event if power supply devices are not responding. The default is Yes.
Event severity when hardware is not responding	Set the event severity level, from 1 to 40, to indicate the importance of an event in which power supply devices are not responding. The default is 15.
Raise event if hardware is not supported?	Select **Yes** to raise an event if power supply devices are not supported, for example do not have SNMP installed, the host is not HP or Dell hardware, or ports are not enabled. The default is Yes.
Event severity when hardware is not supported	Set the event severity level, from 1 to 40, to indicate the importance of an event in which power supply devices are not being supported. The default is 15.
Event severity when HWPowerSupply job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HWPowerSupply job fails unexpectedly. The default is 5.
SNMP Settings	

Parameter	How to Set It
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Monitor Power Supply Status	
Event Notification	
Raise event if device status is "Ok?"	Select **Yes** to raise an event if the status of a power supply device is "Ok". The default is unselected.
Event severity when device status is "Ok"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a power supply device is "Ok". The default is 25.
Raise event if device status is "Degraded?"	Select **Yes** to raise an event if status of a power supply device is "Degraded". The default is Yes.
Event severity when device status is "Degraded"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a power supply device is "Degraded". The default is 15.
Raise event if device status is "Failed" or "Critical?"	Select **Yes** to raise an event if the status of a power supply device is "Failed" or "Critical". The default is Yes.
Event severity when device status is "Failed or "Critical"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a power supply device is "Failed" or "Critical". The default is 10.
Raise event if device status is "Unknown?"	Select **Yes** to raise an event if the status of a power supply device is "Unknown". The default is Yes.
Event severity when device status is "Unknown"	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a power supply device is "Unknown". The default is 15.
Raise event if device status is "Other?"	Select **Yes** to raise an event if the status of a power supply device is "Other". The default is Yes.
Event severity when device status is "Other"	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a power supply device is "Other". The default is 15.
Data Collection	
Collect data for power supply status?	Select **Yes** to collect data for graphs and reports. When enabled, returns a data stream for each SNMP device/SNMP attribute pair. The default is Yes.

HWThermalStatus

Use this Knowledge Script to monitor the state of thermal devices in a system. This script uses the UDP port number to find the thermal device attached to the agent.

The text of an event message indicates the state:

- **Failed**, when a power supply component detects a condition that could permanently damage the system.
- **Degraded**, when a temperature sensor, fan, or other power supply component is outside of normal operating range.
- **Other**, when the status could not be determined or not present.

Prerequisites

- Configure AppManager Security Manager with the information that provides SNMP access to vCenter hosts.
- This script queries the SNMP agent on individual ESX servers and does not depend on vCenter services. If an SNMP port is not enabled by the firewall, run ConfigureHostTraffic to enable a port.

Resource Objects

vCenter host objects

Default Schedule

By default, this script runs every **15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event if hardware is not responding?	Select **Yes** to raise an event if thermal devices are not responding. The default is Yes.
Event severity when hardware is not responding	Set the event severity level, from 1 to 40, to indicate the importance of an event in which thermal devices are not responding. The default is 15.
Raise event if hardware is not supported?	Select **Yes** to raise an event if thermal devices are not supported, for example do not have SNMP installed, the host is not HP or Dell hardware, or ports are not enabled. The default is Yes.
Event severity when hardware is not supported	Set the event severity level, from 1 to 40, to indicate the importance of an event in which thermal devices are not being supported. The default is 15.
Event severity when HWThermalStatus job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the HWThermalStatus job fails unexpectedly. The default is 5.
SNMP Settings	
SNMP port number	Specify the UDP port number to send the SNMP request at each SNMP device. The default value is 161.

Parameter	How to Set It
SNMP retries	Set the number of retries to attempt if a timeout occurs on an SNMP request. The default is 2 retries.
SNMP timeout	Set the number of seconds to wait for a response before timing out an SNMP request. The default is 5 seconds.
Monitor Thermal Device Status	
Event Notification	
Raise event if device status is "Ok" or "Normal?"	Select **Yes** to raise an event if the status of a thermal device is "Ok" or "Normal". The default is unselected.
Event severity when device status is "Ok" or "Normal"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a thermal device is "Ok" or "Normal". The default is 25.
Raise event if device status is "Degraded?"	Select **Yes** to raise an event if status of a thermal device is "Degraded". The default is Yes.
Event severity when device status is "Degraded"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a thermal device is "Degraded". The default is 15.
Raise event if device status is "Failed?"	Select **Yes** to raise an event if the status of a thermal device is "Failed". The default is Yes.
Event severity when device status is "Failed"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the status of a thermal device is "Failed". The default is 10.
Raise event if device status is "Unknown?"	Select **Yes** to raise an event if the status of a thermal device is "Unknown". The default is Yes.
Event severity when device status is "Unknown"	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a thermal device is "Unknown". The default is 15.
Raise event if device status is "Other?"	Select **Yes** to raise an event if the status of a thermal device is "Other". The default is Yes.
Event severity when device status is "Other"	Set the event severity level, from 1 to 40, to indicate the importance of an event in the status of a thermal device is "Other". The default is 15.
Data Collection	
Collect data for thermal device status?	Select **Yes** to collect data for graphs and reports. When enabled, returns a data stream for each SNMP device/SNMP attribute pair. The default is Yes.

ResourcePoolCPUusage

Use this Knowledge Script to monitor CPU usage for the Resource pool. This script raises an event when CPU usage exceeds the threshold. In addition, this script generates data streams for CPU usage in MHz. This script monitors and collects data for the following performance metric:

CPU usage - Sum of actively used virtual CPU of all powered on virtual machines in the resource pool.

Prerequisite

To enable the Knowledge Script to collect accurate CPU usage data for a Resource pool, set the following **Statistics Collection Intervals** appropriately in the vCenter Management Server Configuration:

- **Collection Frequency**: The interval duration in vCenter must be less than or equal to the AppManager job interval schedule. For example, if you run the ResourcePoolCPUusage Knowledge Script at 15-minute intervals, the interval duration in vCenter must be less than or equal to 15 minutes.

For more information about setting the Interval Duration and Statistics Level in the vCenter, see the VMware Virtual Infrastructure 3 documentation.

Resource Object

vCenter-monitored Resource pool

Default Schedule

By default, this script runs every **15 minutes**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when CPU usage exceeds the threshold?	Select **Yes** to raise an event if CPU usage exceeds the threshold you set. The default is Yes.
Event severity when CPU usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 15.
Raise event when Resource pool is either removed or has configuration issues?	Select **Yes** to raise an event if a Resource pool is either removed or has configuration issues. The default is Yes.
Event severity when Resource pool is either removed or has configuration issues	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a Resource pool is either removed or has configuration issues. The default is 15.

Parameter	How to Set It
Event severity when failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when ResourcePoolCPUusage job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ResourcePoolCPUusage job fails unexpectedly. The default is 5.
Data Collection	
Collect data for CPU usage?	Select **Yes** to collect data about CPU usage for charts and reports. The default is unselected.
Monitoring	
Maximum threshold for CPU usage	Specify the maximum amount of CPU usage that can occur before an event is raised. The default is 800 MHz.

ResourcePoolMemUsage

This script monitors memory metrics for the vCenter Resource pool. It raises an event if a monitored metric exceeds the threshold you set. In addition, this script generates a data stream for percentage of memory used and the amount of memory balloon in megabytes per second. This script monitors and collects data for the following performance metrics:

- Memory active - Sum of active memory for all powered-on virtual machines in the resource pool.
- Memory balloon - The sum of values for all memory balloon values for all powered-on virtual machines in the resource pool.
- Memory granted - Sum of all granted memory for all powered-on virtual machines in the resource pool.
- Memory usage - Percentage of available machine memory usage.

Prerequisite

To enable the Knowledge Script to collect accurate memory related data for a Resource pool, set the following **Statistics Collection Intervals** appropriately in the vCenter Management Server Configuration:

- **Collection Frequency**: The interval duration in vCenter must be less than or equal to the AppManager job interval schedule. For example, if you run the ResourcePoolMemUsage Knowledge Script at 15-minute intervals, the interval duration in vCenter must be less than or equal to 15 minutes.

For more information about setting the Interval Duration and Statistics Level in the vCenter, see the VMware Virtual Infrastructure 3 documentation.

Resource Object

vCenter-monitored Resource pool

Default Schedule

By default, this script runs every **15 minutes**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when memory active exceeds the threshold?	Select **Yes** to raise an event when memory active exceeds the threshold you set. The default is unselected.

Parameter	How to Set It
Event severity when memory active exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory active exceeds the threshold you set. The default is 15.
Raise event when memory balloon exceeds the threshold?	Select **Yes** to raise an event when memory balloon exceeds the threshold you set. The default is Yes.
Event severity when memory balloon exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory balloon exceeds the threshold you set. The default is 15.
Raise event when memory granted exceeds the threshold?	Select **Yes** to raise an event when memory granted exceeds the threshold you set. The default is unselected.
Event severity when memory granted exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory granted exceeds the threshold you set. The default is 15.
Raise event when memory usage exceeds the threshold?	Select **Yes** to raise an event when memory usage exceeds the threshold you set. The default is Yes.
Event severity when memory usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold you set. The default is 15.
Raise event when resource pool is either removed or has configuration issues?	Select **Yes** to raise an event when resource pool is either removed or has configuration issues. The default is Yes.
Event severity when resource pool is either removed or has configuration issues	Set the event severity level, from 1 to 40, to indicate the importance of an event in which 4esource pool is either removed or has configuration issues. The default is 15.
Event severity when AppManager failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when AppManager failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when ResourcePoolMemUsage job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ResourcePoolMemUsage job fails unexpectedly. The default is 5.
Data Collection	
Collect data for memory active?	Select **Yes** to collect data about memory active for charts and reports. The default is unselected.
Collect data for memory balloon?	Select **Yes** to collect data about memory balloon for charts and reports. The default is unselected.
Collect data for memory granted?	Select **Yes** to collect data about memory granted for charts and reports. The default is unselected.
Collect data for memory usage?	Select **Yes** to collect data about memory usage for charts and reports. The default is unselected.
Monitoring	
Maximum threshold for memory active	Specify the maximum amount of memory active that can occur before an event is raised. The default is 1024 megabytes.
Maximum threshold for memory balloon	Specify the maximum amount of memory balloon that can occur before an event is raised. The default is 100 kilobytes.
Maximum threshold for memory granted	Specify the maximum amount of memory granted that can occur before an event is raised. The default is 1024 megabytes.
Maximum threshold for memory usage	Specify the maximum amount of memory usage that can occur before an event is raised. The default is 80 percent.

ResourcePoolStatus

Use this Knowledge Script to monitor the overall status of the Resource pool. This script raises an event if the state of the Resource pool changes to one of the following states:

- Inconsistent - One or more nodes in the tree has children whose reservations are greater than the node is configured to support.
- Overcommitted - The tree is consistent internally, but the root resource pool does not have the capacity to meet the reservation of its children.
- Undercommitted - Every node has a reservation greater than the sum of the reservations for its children. There is enough capacity at the root to satisfy all of the resources reserved by the children.

Resource Object

vCenter-monitored Resource pool

Default Schedule

By default, this script runs every **15 minutes**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when Resource pool state changes?	Select **Yes** to raise an event if the Resource pool state changes to inconsistent, overcommitted, or undercommitted. The default is Yes.
Event severity when Resource pool state inconsistent	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Resource pool state changes to inconsistent. The default is 5.
Event severity when Resource pool state overcommitted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Resource pool state changes to overcommitted. The default is 15.
Event severity when Resource pool state undercommitted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Resource pool state changes to undercommitted. The default is 25.
Raise event when Resource pool is removed?	Select **Yes** to raise an event if the Resource pool is removed. The default is Yes.
Event severity when Resource pool is removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Resource pool is removed. The default is 15.
Event severity when failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.

Parameter	How to Set It
Event severity when failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when ResourcePoolStatus job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the ResourcePoolStatus job fails unexpectedly. The default is 5.
Data Collection	
Collect data for state change?	Select **Yes** to collect data for charts and reports. The default is unselected. **Note** When enabled, data collection returns 100 for undercommitted, 50 for overcommitted, and 0 for inconsistent.

ServiceHealthCheck

Use this Knowledge Script to monitor vCenter Server services, such as the vCenter Server Heartbeat service, the vCenter Collector service, and the vCenter Server service. This script raises an event if a service is not running. You can set this script to automatically attempt to start services that are not running.

Note
When you run this script on a proxy agent computer to remotely monitor the vCenter, this script will not monitor the vCenter objects or collect any data.

Resource Object

vCenter servers

Default Schedule

By default, this script runs every **10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Restart VMware Capacity Planner service	Select **Yes** to automatically start the VMware Capacity Planner service when it is not running. The default is unselected.
Restart VMware License Server service?	Select **Yes** to automatically start the VMware License Server service when it is not running. The default is unselected.
Restart VMware Mount service for VirtualCenter service?	Select **Yes** to automatically start the VMware Mount service when it is not running. The default is Yes.
Restart VMware Update Manager service?	Select **Yes** to automatically start the Update Manager service when it is not running. The default is Yes.
Restart VMware vCenter Collector service?	Select **Yes** to automatically start the VMware vCenter Collector service when it is not running. The default is unselected.
Restart VMware vCenter Converter service?	Select **Yes** to automatically start the VMware vCenter Converter service when it is not running. The default is Yes.
Restart VMware vCenter Orchestrator Configuration service?	Select **Yes** to automatically start the VMware Orchestrator Configuration service when it is not running. The default is unselected.
Restart VMware vCenter Server Heartbeat service?	Select **Yes** to automatically start the VMware vCenter Server Heartbeat service when it is not running. The default is unselected.
Restart VMware vCenter Server service?	Select **Yes** to automatically start the VMware vCenter Server service when it is not running. The default is Yes.
Restart VMwareVCMSDS service?	Select **Yes** to automatically start the VMwareVCMSDS service when it is not running. The default is Yes.
Restart VMware VirtualCenter Management Webservices service?	Select **Yes** to automatically start the VMware VirtualCenter Management Webservices service when it is not running. The default is Yes.
Event severity when services restarted	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the vCenter Server services are restarted. The default is 25.

Parameter	How to Set It
Event severity when services not installed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the vCenter Server services are not installed. The default is 25.
Event severity when services not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the vCenter Server services are stopped. The default is 15.
Event severity when services unable to start	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the vCenter Server services are not able to start. The default is 5.

Tasks

Use this Knowledge Script to monitor a set of vCenter tasks. You can filter the tasks by vCenter entity type, task name, and task user name. This script raises an event when monitored task failures are detected. Use the Objects tab to define the resources you want to monitor.

In some instances, a new vCenter task might not include data about the inventory entity associated with the task, such as the VM or the datastore. When this occurs, AppManager associates the task with the root vCenter object in the TreeView. To ensure that you receive events about vCenter tasks that do not contain inventory information, select *Yes* for the *Also raise events on unassociated TreeView objects?* parameter.

Each event report shows the following information:

- Task name
- Target
- User name
- Time on the vCenter Server when the task completed
- Error message

Notes

- The structure of the vCenter Web Service architecture allows you to run only *one* Tasks job on a specific vCenter Server at a time. This limitation prevents the user from starting multiple jobs that monitor the same task failures, which would increase the load on the vCenter Server without any real monitoring benefit. If you have a Tasks job running and try to start another Tasks job, the second job will not complete, and an event message will be raised.
- To avoid long delays when running other VMware Knowledge Scripts, you should only run the Tasks script if your AppManager agent is running on the vCenter server, and not in proxy mode.
- The first time you run this script, you may experience a short delay before actual monitoring begins. This delay is caused by the various initialization processes that must be carried out by the Tasks script.

Resource Objects

Run the Discovery_VirtualCenter Knowledge Script on the objects you want to monitor before running this Knowledge Script. You can also monitor objects that the Discovery_VirtualCenter Knowledge Script does *not* discover, such as distributed virtual port groups and distributed virtual switches.

- vCenter server
- Clusters
- Datacenters
- Datastores
- Hosts
- Resource pools
- Virtual machines
- Folders (you can only monitor the folder objects found under the Host & Clusters parent folder in the TreeView pane)
- Distributed virtual port groups (not displayed in the TreeView pane)

- Distributed virtual switches (not displayed in the TreeView pane)
- Network (not displayed in the TreeView pane)

Default Schedule

The default interval for this script is **Asynchronous**. Regardless of the schedule you select, once you start the Knowledge Script, its job status appears as **Running**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when AppManager failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in. The default is 5.
Event severity when Tasks job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Tasks job fails unexpectedly. The default is 5.
Event severity when filter settings contain conflicts	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the filter settings contain conflicts. The default is 15.
Additional Settings	
Event Details	
Event detail format	Select either **HTML Table** or **Plain Text** as the format for event detail. The default is HTML Table.
Monitor vCenter Task Failures	
Event Notification	
Raise event if vCenter task fails?	Select **Yes** to raise an event if a vCenter "error" event is detected. The default is Yes.
Event severity when vCenter task fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a vCenter task fails. The default is 10.
Select vCenter entity type	Click **Browse [...]** to select the vCenter entity type you want to monitor. The default is all entity types: Datacenter,Datastore,Cluster,Folder,HostSystem,ResourcePool,VirtualMachine
Task user name	If you want to raise events only for a specific user, provide the name of the vCenter user you want to monitor. If you do not enter a user name, AppManager raises events related to all users. This parameter is *not* case-sensitive. The asterisk (*) and (?) are acceptable wildcards.
Task name	If you want to raise events only for a specific task, provide the name of the vCenter task you want to monitor. If you do not enter a task name, AppManager raises events related to all tasks. This parameter is *not* case-sensitive. The asterisk (*) and (?) are acceptable wildcards.
Also raise events on unassociated TreeView objects?	Select **Yes** to raise an event for unassociated objects in the TreeView pane, including vCenter tasks that do not contain inventory information. The default is unselected.

VirtualCenterCPUUsage

Use this Knowledge Script to monitor the CPU usage of the vCenter process and total CPU usage on the computer hosting the vCenter. This script raises an event when CPU usage exceeds the threshold you set. This script monitors and collects data for the following performance metric:

- CPU usage - Amount of actively used virtual CPU, as a percentage of total available CPU.

Note
When you run this script on a proxy agent computer to remotely monitor the vCenter, this script will not monitor the vCenter objects or collect any data.

Resource Object

vCenter servers

Default Schedule

By default, this script runs every **10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when VirtualCenter CPU usage exceeds the threshold?	Select **Yes** to raise an event if vCenter CPU usage exceeds the threshold you set. The default is Yes.
Event severity when VirtualCenter CPU usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU usage for the vCenter process exceeds the threshold. The default is 15.
Raise event when total host CPU usage exceeds the threshold?	Select **Yes** to raise an event if total CPU usage on the host computer exceeds the threshold you set. The default is Yes.
Event severity when total host CPU usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which total CPU usage on the host computer exceeds the threshold. The default is 15.
Event severity when VirtualCenter CPUusage job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the vCenter CPUusage job fails unexpectedly. The default is 5.
Data Collection	
Collect data for VirtualCenter CPU usage?	Select **Yes** to collect data about vCenter CPU usage charts and reports. The default is unselected.
Collect data for total host CPU usage?	Select **Yes** to collect data about total CPU usage on the host for charts and reports. The default is unselected.
Monitoring	
Maximum threshold for VirtualCenter CPU usage (%)	Specify the maximum amount of CPU usage that can occur for the vCenter process before an event is raised. The default is 60%.
Maximum threshold for total host CPU usage (%)	Specify the maximum amount of CPU usage that can occur on the host computer before an event is raised. The default is 95%.

VirtualCenterMemoryUsage

Use this Knowledge Script to monitor memory usage of the vCenter process and the total amount of memory being used on the server hosting vCenter. This script raises an event if the memory usage exceeds the threshold you set.

Note
When you run this script on a proxy agent computer to remotely monitor the vCenter, this script will not monitor the vCenter objects or collect any data.

Resource Object

vCenter servers

Default Schedule

By default, this script runs every **10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when memory usage exceeds the threshold?	Select **Yes** to raise an event if the percentage of cluster memory usage exceeds the threshold you set. The default is Yes.
Event severity when memory usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. The default is 15.
Raise event when total host memory usage exceeds the threshold?	Select **Yes** to raise an event if total memory usage for the host computer exceeds the threshold you set. The default is Yes.
Event severity when total host memory usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which total memory usage for the host computer exceeds the threshold. The default is 15.
Event severity when VirtualCenterMemoryUsage job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VirtualCenterMemoryUsage job fails unexpectedly. The default is 5.
Data Collection	
Collect data for VirtualCenter memory usage?	Select **Yes** to collect data about vCenter memory usage for charts and reports. The default is unselected.
Collect data for total host memory usage?	Select **Yes** to collect data about total memory usage on the host computer for charts and reports. The default is unselected.
Monitoring	
Maximum threshold for VirtualCenter memory usage (KB)	Specify the maximum amount of memory usage that can occur for the vCenter process before an event is raised. The default is 20000 kilobytes.
Maximum threshold for total host memory usage (KB)	Specify the maximum amount of memory usage that can occur on the host computer before an event is raised. The default is 20000 kilobytes.

VirtualMachineInventory

Use this Knowledge Script to monitor virtual machines that are added, removed, renamed, moved, or migrated within vCenter. This script raises an event when any of the listed actions occurs. In addition, this script can perform a rediscovery when these events occur, which allows the AppManager console to display the most current inventory of virtual machines in vCenter.

Resource Object

vCenter servers

Default Schedule

By default, this script runs every **hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when virtual machines added?	Select **Yes** to raise an event when a virtual machine is added to vCenter. The default is Yes.
Event severity when virtual machines added	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a virtual machine is added to vCenter. The default is 15.
Raise event when virtual machines removed?	Select **Yes** to raise an event when a virtual machine is removed is removed from vCenter. The default is Yes.
Event severity when virtual machines removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a virtual machine is removed from vCenter. The default is 15.
Raise event when virtual machines renamed?	Select **Yes** to raise an event when a virtual machine is renamed. The default is Yes.
Event severity when virtual machines renamed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a virtual machine is renamed. The default is 15.
Raise event when virtual machines moved?	Select **Yes** to raise an event when a virtual machine is moved within vCenter. The default is unselected.
Event severity when virtual machines moved	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a virtual machines is moved within vCenter. The default is 15.
Raise event when virtual machines migrated?	Select **Yes** to raise an event when a virtual machine is migrated within vCenter. The default is Yes.
Event severity when virtual machines migrated	Set the event severity level, from 1 to 40, to indicate the importance of an event in which virtual machines are migrated within vCenter. The default is 15.
Raise event when rediscovery failed?	Select **Yes** to raise an event when rediscovery failed. The default is unselected.
Event severity when rediscovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which rediscovery fails. The default is 5.

Parameter	How to Set It
Event severity when failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when VirtualMachineInventory job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VirtualMachineInventory job fails unexpectedly. The default is 5.
Data Collection	
Collect data when virtual machines added?	Select **Yes** to collect data about virtual machines that are added to vCenter. The default is unselected.
Collect data when virtual machines removed?	Select **Yes** to collect data about virtual machines that are removed from vCenter. The default is unselected.
Collect data when virtual machines renamed?	Select **Yes** to collect data about virtual machines that are renamed within vCenter. The default is unselected.
Collect data when virtual machines moved?	Select **Yes** to collect data about virtual machines that are moved within vCenter. The default is unselected.
Collect data when virtual machines migrated?	Select **Yes** to collect data about virtual machines that are migrated in vCenter. The default is unselected.
Rediscovery Options	
Rediscover if virtual machines added?	Select **Yes** to perform rediscovery when a virtual machine is added to vCenter. The default is unselected.
Rediscover if virtual machines removed?	Select **Yes** to perform rediscovery when a virtual machine is removed from vCenter. The default is unselected.
Rediscover if virtual machines renamed?	Select **Yes** to perform rediscovery when a virtual machine is renamed within vCenter. The default is unselected.
Rediscover if virtual machines moved?	Select **Yes** to perform rediscovery when a virtual machine is moved within vCenter. The default is unselected.
Rediscover if virtual machines migrated?	Select **Yes** to perform rediscovery when a virtual machine is migrated in vCenter. The default is unselected.

VmConnected

Use this Knowledge Script to monitor changes in the connection status of virtual machines to vCenter. This script raises an event if a virtual machine is disconnected or reconnected.

Resource Object

vCenter-monitored virtual machine

Default Schedule

By default, this script runs every day at 15 minute intervals starting at 12:01 AM and ending at 11:59 PM. If you start the job after the scheduled starting time, the script runs at the time of the next scheduled interval. For example, if you start the job at 12:10 AM, it runs for the first time at 12:16 AM.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event when a virtual machine removed?	Select **Yes** to raise an event when virtual machine is removed. The default is unselected.
Event severity when a virtual machine is removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a virtual machine is removed. The default is 15.
Event severity when AppManager failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when VmConnected job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VmConnected job fails unexpectedly. The default is 5.
Additional Settings	
Event Details	
Event detail format	Select either **HTML Table** or **Plain Text** as the format for event detail. The default is HTML Table.
Monitor Connection Status	
Event Notification	
Raise event when a virtual machine is disconnected	Select **Yes** to raise an event when a connected virtual machine is disconnected from vCenter. The default is Yes.

Parameter	How to Set It
Event Severity when virtual machine is disconnected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a virtual machine is disconnected from vCenter. The default is 15.
Raise event when a virtual machine is reconnected	Select **Yes** to raise an event when a disconnected virtual machine is reconnected to vCenter. The default is Yes.
Event severity when virtual machine is reconnected	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a virtual machine is reconnected to vCenter. The default is 15.

VmCPUusage

Use this Knowledge Script to monitor the following metrics for a virtual machine on a vCenter host:

- CPU ready - Percentage of time that the virtual machine was ready, but could not get scheduled to run on the physical CPU. CPU ready time is dependent on the number of virtual machines on the host and their CPU loads.
- CPU system - Amount of time spent on system processes on each virtual CPU in the virtual machine.
- CPU usage - Amount of actively used virtual CPU, as a percentage of total available CPU. This is the host's view of the CPU usage, not the guest operating system's view. It is the average CPU utilization over all available virtual CPUs in the virtual machine.
- CPU usage in MHz - Total amount of CPU used, in MHz, during the interval. This is the same value as CPU usage represented in MHz instead of a percentage.
- CPU used - Total CPU usage. CPU used as a percentage and CPU usage as a percentage are the same value.
- CPU wait - Amount of CPU time spent in wait state.

This script raises an event if a monitored value exceeds the threshold you set.

If this script is running in addition to the disk I/O, memory usage, or network I/O scripts, you should instead run the VmCPUusage, VmMemoryUsage, VmDiskIO, and VmNetworkIO Knowledge Scripts to optimize resource usage on the vCenter host.

Notes

- CPU wait is a combined metric that includes CPU idle, CPU wait, and CPU halted. CPU wait is a defect in VMware. NetIQ Corporation is currently researching a solution with VMware (SR #1123183421). AppManager matches the value provided by VMware. For more information about this issue, see the VI SDK Release Notes at http://www.vmware.com/support/developer/vc-sdk/visdk-2.5.0-200711-releasenotes.html.
- In vCenter version 2.0.2 environments, event and datastream values for the CPU Wait metric correspond to the value of the CPU Idle metric.

Resource Object

vCenter-monitored virtual machine

Default Schedule

By default, this script runs every day at 15 minute intervals starting at 12:05 AM and ending at 11:59 PM. If you start the job after the scheduled starting time, the script runs at the time of the next scheduled interval. For example, if you start the job at 12:10 AM, it runs for the first time at 12:20 AM.

Note

If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Job Failure Notification	
Raise event when CPU metrics are not available?	Select **Yes** to raise an event if CPU metrics are not available. The default is unselected.
Event severity when CPU metrics are not available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which CPU metrics are not available. The default is 15.
Event severity when AppManger failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when AppManager failed to log in	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when VmCPUUsage job fails unexpectedly	Set the severity level, from 1 to 40, to indicate the importance of an event in which the VmCPUUsage job fails unexpectedly. The default is 5.
Additional Settings	
Event Details	
Event detail format	Select either **HTML Table** or **Plain Text** as the format for event detail. The default is HTML Table.
Monitoring CPU Ready	
Event Notification	
Raise event when average CPU ready exceeds the threshold?	Select **Yes** to raise an event when average CPU ready exceeds the threshold you set. The default is Yes.
Threshold -- Maximum average CPU ready	Specify the maximum average CPU ready that can occur before an event is raised. The default is 10 percent.
Event severity when average CPU ready exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event when average CPU ready exceeds the threshold. The default is 15.
Data Collection	
Collect data for average CPU ready?	Select **Yes** to collect data about average CPU ready for charts and reports. The default is unselected.
Collect data for individual CPU ready?	Select **Yes** to collect data about individual CPU ready for charts and reports. The default is unselected.
Monitoring CPU System	
Event Notification	
Raise event when average CPU system exceeds the threshold?	Select **Yes** to raise an event when average CPU system exceeds the threshold you set. The default is unselected.
Threshold -- Maximum average CPU system	Specify the maximum average CPU system that can occur before an event is raised. The default is 20 percent.
Event severity when average CPU system exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event when average CPU system exceeds the threshold. The default is 15.
Raise event when individual CPU system exceeds the threshold?	Select **Yes** to raise an event when individual CPU system exceeds the threshold you set. The default is unselected.
Threshold -- Maximum individual CPU system	Specify the maximum individual CPU system that can occur before an event is raised. The default is 20 percent.

Parameter	How to Set It
Event severity when individual CPU system exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event when individual CPU system exceeds the threshold. The default is 15.
Data Collection	
Collect data for average CPU system?	Select **Yes** to collect data about average CPU system for charts and reports. The default is unselected.
Collect data for individual CPU system?	Select **Yes** to collect data about individual CPU system for charts and reports. The default is unselected.
Monitoring CPU Usage	
Event Notification	
Raise event when average CPU usage exceeds the threshold?	Select **Yes** to raise an event when average CPU usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum average CPU usage	Specify the maximum average CPU usage that can occur before an event is raised. The default is 80 percent.
Event severity when average CPU usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event when average CPU usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for average CPU usage?	Select **Yes** to collect data about average CPU usage for charts and reports. The default is unselected.
Collect data for individual CPU usage?	Select **Yes** to collect data about individual CPU usage for charts and reports. The default is unselected.
Monitoring CPU Usage in MHz	
Event Notification	
Raise event when average CPU usage in MHz exceeds the threshold?	Select **Yes** to raise an event when average CPU usage in MHz exceeds the threshold you set. The default is unselected.
Threshold -- Maximum average CPU usage in MHz	Specify the maximum average CPU usage in MHz that can occur before an event is raised. The default is 2000 MHz.
Event severity when average CPU usage in MHz exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event when average CPU usage in MHz exceeds the threshold. The default is 15.
Raise event when individual CPU usage in MHz exceeds the threshold?	Select **Yes** to raise an event when individual CPU usage in MHz exceeds the threshold you set. The default is unselected.
Threshold -- Maximum individual CPU usage in MHz	Specify the maximum individual CPU usage in MHz that can occur before an event is raised. The default is 2000 MHz.
Event severity when individual CPU usage in MHz exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event when individual CPU usage in MHz exceeds the threshold. The default is 15.
Data Collection	
Collect data for average CPU usage in MHz?	Select **Yes** to collect data about average CPU usage in MHz for charts and reports. The default is unselected.
Collect data for individual CPU usage in MHz?	Select **Yes** to collect data about individual CPU usage in MHz for charts and reports. The default is unselected.
Monitoring CPU Used	
Event Notification	
Raise event when average CPU used exceeds the threshold?	Select **Yes** to raise an event when average CPU used exceeds the threshold you set. The default is Yes.
Threshold -- Maximum average CPU used	Specify the maximum average CPU used that can occur before an event is raised. The default is 80 percent.

Parameter	How to Set It
Event severity when average CPU used exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event when average CPU used exceeds the threshold. The default is 15.
Data Collection	
Collect data for average CPU used?	Select **Yes** to collect data about average CPU used for charts and reports. The default is unselected.
Collect data for individual CPU used?	Select **Yes** to collect data about individual CPU used for charts and reports. The default is unselected.
Monitoring CPU Wait	
Event Notification	
Raise event when average CPU wait exceeds the threshold?	Select **Yes** to raise an event when average CPU wait exceeds the threshold you set. The default is unselected.
Threshold -- Maximum average CPU wait	Specify the maximum average CPU wait that can occur before an event is raised. The default is 10 percent.
Event severity when average CPU wait exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event when average CPU wait exceeds the threshold. The default is 15.
Data Collection	
Collect data for average CPU wait?	Select **Yes** to collect data about average CPU wait for charts and reports. The default is unselected.
Collect data for individual CPU wait?	Select **Yes** to collect data about individual CPU wait for charts and reports. The default is unselected.

VmDiskIO

Use this Knowledge Script to monitor disk reads/writes for a virtual machine. This script raises an event if the rate of reads/writes exceeds the threshold you set. This script monitors and collects data for the following performance metrics:

- Disk read rate - Rate at which data is read from each virtual disk on the virtual machine.
- Disk write rate - Rate at which data is written to each virtual disk on the virtual machine.

If this script is running in addition to the CPU usage, Memory usage, or Network I/O scripts, you should instead run the VmCPUusage, VmMemoryUsage, VmDiskIO, and VmNetworkIO Knowledge Scripts to optimize the resource usage on the vCenter host.

Resource Object

vCenter-monitored virtual machine

Default Schedule

By default, this script runs every day at 15 minute intervals starting at 12:07 AM and ending at 11:59 PM. If you start the job after the scheduled starting time, the script runs at the time of the next scheduled interval. For example, if you start the job at 12:10 AM, it runs for the first time at 12:22 AM.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when total disk IO exceeds the threshold?	Select **Yes** to raise an event when total disk IO exceeds the threshold you set. The default is unselected.
Event severity when total disk IO exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which total disk IO exceeds the threshold you set. The default is 15
Raise event when average disk reads exceed the threshold?	Select **Yes** to raise an event when average disk reads exceed the threshold you set. The default is Yes.
Event severity when average disk reads exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which average disk reads exceed the threshold. The default is 15.
Raise event when disk writes exceed the threshold?	Select **Yes** to raise an event if the rate of disk writes exceeds the threshold you set. The default is Yes.
Event severity when disk writes exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which disk writes exceeds the threshold. The default is 15.
Raise event when disk I/O metrics are not available?	Select **Yes** to raise an event if disk I/O metrics are not available. The default is unselected.

Parameter	How to Set It
Event severity when disk I/O metrics are not available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which disk I/O metrics are not available. The default is 15.
Event severity when AppManager failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when AppManager failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when VmDiskIO job fails unexpectedly.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VmDiskIO job fails unexpectedly. The default is 5.
Data Collection	
Collect data for total disk IO?	Select **Yes** to collect data about total disk IO for charts and reports. The default is unselected.
Collect data for average disk reads?	Select **Yes** to collect data about average disk reads for charts and reports. The default is unselected.
Collect data for average disk writes?	Select **Yes** to collect data about average disk writes for charts and reports. The default is unselected.
Monitoring	
Maximum threshold for disk IO	Specify the maximum rate at which disk IO can occur before an event is raised. The default is 20 megabytes per second.
Maximum threshold for average disk reads	Specify the maximum rate at which average disk reads can occur before an event is raised. The default is 1 megabyte per second.
Maximum threshold for average disk writes	Specify the maximum rate at which average disk writes can occur before an event is raised. The default is 1 megabyte per second.

VmDiskUsage

Use this Knowledge Script to monitor logical disk usage for a virtual machine. This script raises an event disk usage exceeds the threshold you set.

This Knowledge Script cannot monitor the logical disk usage for a virtual machine when the virtual machine's disk is a mounted drive.

Resource Object

vCenter-monitored virtual machine

Default Schedule

By default, this script runs every **15 minutes**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event when disk metrics are not available?	Select **Yes** to raise an event when disk metrics are not available. The default is unselected.
Event severity when disk metrics are not available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which disk metrics are not available. The default is 15.
Raise event when virtual machine is either deleted or removed?	Select **Yes** to raise an event when the Virtual Machine is either deleted or removed. The default is unselected.
Event severity when virtual machine is either deleted or removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the virtual machine is either deleted or removed. The default is 15.
Event severity when AppManager failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to get metrics. The default is 15.
Event severity when AppManager failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in. The default is 5.
Event severity when VMDiskUsage job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VMDiskUsage job fails unexpectedly. The default is 5.
Additional Settings	
Event Details	

Parameter	How to Set It
Event detail format	Select either **HTML Table** or **Plain Text** as the format for event detail. The default is HTML Table.
Monitor Logical Disk Usage	
Event Notification	
Raise event if logical disk free space falls below the threshold	Select **Yes** to raise an event when logical disk free space falls below the threshold you set. The default is Yes.
Unit type	Select whether to measure the amount of logical disk free space in **Percent** or **MBytes**. The default is MBytes.
Threshold -- Minimum logical disk free space available	Specify the minimum amount of logical disk free space that can be available before an event is raised. The default is 500 Mbytes.
Event severity when logical disk free space falls below the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which logical disk available free space falls below the threshold. The default is 15.
Raise event if logical disk space usage exceeds the threshold	Select **Yes** to raise an event when logical disk space usage exceeds the threshold you set. The default is Yes.
Unit type	Select whether to measure the amount of disk space usage in **Percent** or **MBytes**. The default is Percent.
Threshold -- Maximum logical disk space usage	Specify the amount of logical disk space usage that can occur before an event is raised. The default is 80 percent.
Event severity when logical disk space usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which logical disk space usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for logical disk free space?	Select **Yes** to collect data about logical disk free space for charts and reports. The default is unselected.
Collect data for logical disk space usage?	Select **Yes** to collect data about logical disk space usage for charts and reports. The default is unselected.

VmMemoryUsage

Use this Knowledge Script to monitor memory usage for a virtual machine. This script raises an event if a monitored metric exceeds the threshold you set. This script monitors and collects data for the following performance metrics:

- Memory active - Amount of guest physical memory in use by the virtual machine. This is an estimate provided by the VMkernel and represents the actual amount of memory the virtual machine needs.
- Memory balloon - Amount of guest physical memory that is currently reclaimed from the virtual machine through ballooning. This is the amount of guest physical memory that has been allocated and pinned by the balloon driver.
- Memory consumed - Amount of guest physical memory consumed by the virtual machine for guest memory. Consumed memory does not include overhead memory. It includes shared memory and memory that might be reserved, but not actually used.
- Memory granted - Guest "physical" memory that is mapped to machine memory.
- Memory overhead - Amount of overhead memory (in kilobytes) required for virtualization of the virtual machine. Excess memory overhead values can indicate virtualization problems.
- Memory shared - Amount of guest "physical" memory shared with other virtual machines (through the VMkernel's transparent page-sharing mechanism, a RAM de-duplication technique).
- Memory state - Amount of free machine memory on the host. The VMkernel has four free-memory thresholds that affect memory reclamation:
  - 0 (high) Free memory ≥ 6% of machine memory minus Service Console memory.
  - 1 (soft) 4%
  - 2 (hard) 2%
  - 3 (low) 1%
  - 0 (high) and 1 (soft): Swapping is favored over ballooning.
  - 2 (hard) and 3 (low): Ballooning is favored over swapping.
- Memory swap in - Total amount of data that has been read into machine memory from the swap file since the virtual machine was powered on.
- Memory swap in rate - Rate at which memory is swapped from disk into active memory.
- Memory swap out - Total amount of data that the VMkernel has written to the virtual machine's swap file from machine memory. This statistic refers to VMkernel swapping and not to guest OS swapping.
- Memory swap out rate - Rate at which memory is being swapped from active memory to disk.
- Memory usage - Percentage of total configured or available memory usage.
- Memory zero - Memory (as a percentage) that is zeroed out. This value can indicate that there are virtual machines with more memory allocated to them than they need. By reducing the allocated memory you can increase the total number of running virtual machines, achieving a greater virtual to physical running ratio.

If this script is running in addition to the Disk I/O, CPU usage, or Network I/O scripts, instead run the VmCPUusage, VmMemoryUsage, VmDiskIO, and VmNetworkIO Knowledge Scripts to optimize the resource usage on the vCenter host.

Resource Object

vCenter-monitored virtual machine

Default Schedule

By default, this script runs every day at 15 minute intervals starting at 12:03 AM and ending at 11:59 PM. If you start the job after the scheduled starting time, the script runs at the time of the next scheduled interval. For example, if you start the job at 12:10 AM, it runs for the first time at 12:18 AM.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Raise event when memory metrics are not available?	Select **Yes** to raise an event if memory metrics are not available. The default is unselected.
Event severity when memory metrics are not available	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory metrics are not available. The default is 15.
Event severity when AppManager failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when AppManager failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when VmMemoryUsage job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VmMemoryUsage job fails unexpectedly. The default is 5.
Additional Settings	
Event Details	
Event detail format	Select either **HTML Table** or **Plain Text** as the format for event detail. The default is HTML Table.
Monitoring Memory Active	
Event Notification	
Raise event when memory active exceeds the threshold?	Select **Yes** to raise an event when the memory active exceeds the threshold you set. The default is unselected.
Threshold -- Maximum for memory active	Specify the maximum percentage for memory active before an event is raised. The default is 20 percent.
Event severity when memory active exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event when the active memory exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory active?	Select **Yes** to collect data about memory active for charts and reports. The default is unselected.
Monitor Memory Balloon	
Event Notification	

Parameter	How to Set It
Raise event when memory balloon exceeds the threshold?	Select **Yes** to raise an event if the percentage of memory balloon exceeds the threshold you set. The default is Yes.
Threshold -- Maximum memory balloon	Specify the maximum percentage for memory balloon before an event is raised. The default is 2 percent.
Event severity when memory balloon exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of memory balloon exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory balloon?	Select **Yes** to collect data about memory balloon for charts and reports. The default is unselected.
Monitor Memory Consumed	
Event Notification	
Raise event when memory consumed exceeds the threshold?	Select **Yes** to raise an event if the percentage of memory consumed exceeds the threshold you set. The default is Yes.
Threshold -- Maximum memory consumed	Specify the maximum percentage of memory consumed before an event is raised. The default is 80 percent.
Event severity when memory consumed exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of memory consumed exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory consumed?	Select **Yes** to collect data about memory consumed for charts and reports. The default is unselected.
Monitor Memory Granted	
Event Notification	
Raise event when memory granted exceeds the threshold?	Select **Yes** to raise an event when the amount of memory granted exceeds the threshold you set. The default is unselected.
Threshold -- Maximum memory granted	Specify the maximum amount of memory granted before an event is raised. The default is 1024 megabytes.
Event severity when memory granted exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of memory granted exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory granted?	Select **Yes** to collect data about memory granted for charts and reports. The default is unselected.
Monitor Memory Overhead	
Event Notification	
Raise event when memory overhead exceeds the threshold?	Select **Yes** to raise an event when the amount of memory overhead exceeds the threshold you set. The default is unselected.
Threshold --Maximum memory overhead	Specify the maximum amount of memory overhead that can occur before an event is raised. The default is 100 megabytes.
Event severity when memory overhead exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of memory shared falls below the threshold. The default is 15.
Data Collection	
Collect data for memory overhead?	Select **Yes** to collect data about memory overhead for charts and reports. The default is unselected.
Monitor Memory Shared	
Event Notification	

Parameter	How to Set It
Raise event when memory shared falls below the threshold?	Select **Yes** to raise an event when the amount of memory shared falls below the threshold you set. The default is unselected.
Threshold --Maximum memory shared	Specify the maximum amount of memory shared that can occur before an event is raised. The default is 50 megabytes.
Event severity when memory shared exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of memory shared falls below the threshold. The default is 15.
Data Collection	
Collect data for memory shared?	Select **Yes** to collect data about memory shared for charts and reports. The default is unselected.
Monitor Memory State	
Event Notification	
Raise event when memory state is hard?	Select **Yes** to raise an event when the memory state is hard. The default is unselected.
Event severity when memory state is hard	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the memory state is hard. The default is 10.
Raise event when memory state is high?	Select **Yes** to raise an event when the memory state is high. The default is unselected.
Event severity when memory state is high	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the memory state is high. The default is 25.
Raise event when memory state is low?	Select **Yes** to raise an event when the memory state is low. The default is unselected.
Event severity when memory state is low	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the memory state is low. The default is 5.
Raise event when memory state is soft?	Select **Yes** to raise an event when memory state is soft. The default is unselected.
Event severity when memory state is soft	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the memory state is soft. The default is 15.
Data Collection	
Collect data for memory state?	Select **Yes** to collect data about memory state for charts and reports. The default is unselected.
Monitor Memory Swap In	
Data Collection	
Collect data for memory swap in?	Select **Yes** to collect data about memory swap in for charts and reports. The default is unselected.
Monitor Memory Swap In Rate	
Event Notification	
Raise event when memory swap in rate exceeds the threshold?	Select **Yes** to raise an event when the memory swap in rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum memory swap in rate	Specify the maximum memory swap in rate that can occur before an event is raised. The default is 1 megabyte per second.
Event severity when memory swap in rate exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the memory swap in rate exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for memory swap in rate?	Select **Yes** to collect data about memory swap in rate for charts and reports. The default is unselected.
Monitor Memory Swap Out	
Data Collection	
Collect data for memory swap out?	Select **Yes** to collect data about memory swap out for charts and reports. The default is unselected.
Monitor Memory Swap Out Rate	
Event Notification	
Raise event when memory swap out rate exceeds the threshold?	Select **Yes** to raise an event when the memory swap out rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum memory swap out rate	Specify the maximum memory swap out rate that can occur before an event is raised. The default is 1 megabyte per second.
Event severity when memory swap out rate exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the memory swap out rate exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory swap out rate?	Select **Yes** to collect data about memory swap out rate for charts and reports. The default is unselected.
Monitor Memory Usage	
Event Notification	
Raise event when memory usage exceeds the threshold?	Select **Yes** to raise an event when memory usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum memory usage	Specify the maximum memory usage that can occur before an event is raised. The default is 80 percent.
Event severity when memory usage exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory usage?	Select **Yes** to collect data about memory usage for charts and reports. The default is unselected.
Monitor Memory Zero	
Event Notification	
Raise event when memory zero exceeds the threshold?	Select **Yes** to raise an event when memory zero exceeds the threshold you set. The default is unselected.
Threshold -- Maximum memory zero	Specify the maximum memory zero that can occur before an event is raised. The default is 20 percent.
Event severity when memory zero exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which memory zero exceeds the threshold. The default is 15.
Data Collection	
Collect data for memory zero?	Select **Yes** to collect data about memory zero for charts and reports. The default is unselected.

VmNetworkIO

Use this Knowledge Script to monitor network reads/writes for a virtual machine. This script raises an event if the rate of network reads/writes exceed the threshold you set. This script monitors and collects data for the following performance metrics:

- Network reads - The rate at which data is received across the virtual machine's vNIC (virtual network interface controller).
- Network writes (Network I/O) - The rate at which data is transmitted across the virtual machine's vNIC (virtual network interface controller).

Resource Object

vCenter-monitored virtual machine

Default Schedule

By default, this script runs every day at 15 minute intervals starting at 12:09 AM and ending at 11:59 PM. If you start the job after the scheduled starting time, the script runs at the time of the next scheduled interval. For example, if you start the job at 12:10 AM, it runs for the first time at 12:24 AM.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when network reads exceed the threshold?	Select **Yes** to raise an event if the rate of network reads exceeds the threshold you set. The default is Yes.
Event severity when network reads exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the rate of network reads exceeds the threshold. The default is 15.
Raise event when individual network reads exceed the threshold?	Select **Yes** to raise an event if the rate of individual network reads exceeds the threshold you set. The default is unselected.
Event severity when individual network reads exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the rate of individual network reads exceeds the threshold. The default is 15.
Raise event when network writes exceed the threshold?	Select **Yes** to raise an event if the rate of network writes exceeds the threshold you set. The default is Yes.
Event severity when network writes exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the rate of network reads exceeds the threshold. The default is 15.
Raise event when individual network writes exceed the threshold?	Select **Yes** to raise an event if the rate of individual network writes exceed the threshold you set. The default is unselected.

Parameter	How to Set It
Event severity when individual network writes exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the rate of individual network reads exceed the threshold. The default is 15.
Raise event when network I/O metrics are not available?	Select **Yes** to raise an event if network I/O metrics are not available. The default is unselected.
Event severity network I/O metrics are not available.	Set the event severity level, from 1 to 40, to indicate the importance of an event in which network I/O metrics are not available. The default is 15.
Event severity when AppManager failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when AppManager failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when VmNetworkI/O job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VmNetworkIO job fails unexpectedly. The default is 5.
Data Collection	
Collect data for network reads?	Select **Yes** to collect data about the rate of network reads for charts and reports. The default is unselected.
Collect data for individual network reads?	Select **Yes** to collect data about the rate of individual network reads for charts and reports. The default is unselected.
Collect data for network writes?	Select **Yes** to collect data about the rate of network writes for charts and reports. The default is unselected.
Collect data for network individual writes?	Select **Yes** to collect data about the rate of individual network writes for charts and reports. The default is unselected.
Monitoring	
Maximum threshold for network reads	Specify the maximum rate at which network reads can occur before an event is raised. The default is 1 Mbit per second.
Maximum threshold for individual network reads	Specify the maximum rate at which individual network reads can occur before an event is raised. The default is 1 Mbit per second.
Maximum threshold for network writes	Specify the maximum rate at which network writes can occur before an event is raised. The default is 1 Mbit per second.
Maximum threshold for individual network writes	Specify the maximum rate at which individual network writes can occur before an event is raised. The default is 1 Mbit per second.

VmPowerStatus

Use this Knowledge Script to monitor changes in the power status of virtual machines. This script raises an event if a virtual machine is powered on, powered off, or suspended. Based on these events, you can choose to restart, stop, or resume the monitored virtual machines.

Prerequisite

Enable Power On, Power Off, Suspend, and Restart permissions to run this Knowledge Script. For more information, see "Upgrading Knowledge Script Jobs" on page 13.

Resource Object

vCenter-monitored virtual machine

Default Schedule

By default, this script runs every **15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Raise event when virtual machine powered on?	Select **Yes** to raise an event when a virtual machine is in the "powered on" state. The default is Yes.
Event severity when virtual machine powered on	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a virtual machine is in the "powered on" state. The default is 15.
Raise event when virtual machine powered off?	Select **Yes** to raise an event when a virtual machine is in the "powered off" state. The default is Yes.
Event severity when virtual machine powered off	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the virtual machine is in the "powered off" state. The default is 15.
Raise event when virtual machine suspended?	Select **Yes** to raise an event when a virtual machine is in "suspended" state. The default is Yes.
Event severity when virtual machine suspended	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a virtual machine is in "suspended" state. The default is 15.
Raise event when virtual machine is either disconnected or removed?	Select **Yes** to raise an event when a virtual machine is either disconnected or removed. The default is Yes.
Event severity when virtual machine either disconnected or removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a virtual machine is either disconnected or removed. The default is 15.
Event severity when failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity when failed to log in	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.

Parameter	How to Set It
Event severity when VmPowerStatus job fails unexpectedly	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VmPowerStatus job fails unexpectedly. The default is 5.
Actions	
When a “powered on” event raised, perform this action	Choose to **power off**, **suspend**, or take **no action** when an event is raised because the virtual machine is in “powered on” state. The default is no action.
When a “powered off” event raised, perform this action	Choose to **power on** or take **no action** when an event is raised because the virtual machine is in “powered off” state. The default is power on.
When a “suspended” event raised, perform this action	Choose to **resume** or take **no action** when an event is raised because the virtual machine is in “suspended” state. The default is no action.

VmToolsStatus

Use this Knowledge Script to monitor the status of VMware Tools for virtual machines. This script raises an event if VMware Tools was not installed, is not running, or has an outdated version.

Resource Object

vCenter-monitored virtual machine

Default Schedule

By default, this script runs every **1 Day**.

Note
If you are running this script as part of the Recommended Knowledge Script Groups, do not change the schedule. The schedules for the recommended scripts are staggered to lessen the impact on CPU utilization when you run the KSG.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when AppManager failed to get metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager failed to retrieve host connection status from vCenter. The default is 15.
Event severity AppManager when failed to log in	Set the event severity level, form 1 to 40, to indicate the importance of an event in which AppManager failed to log in to vCenter. The default is 5.
Event severity when VMToolsStatus job fails unexpectedly	Set the event severity level, form 1 to 40, to indicate the importance of an event in which the VMToolsStatus job fails unexpectedly. The default is 5.
Raise event when virtual machine is either disconnected or removed?	Select Yes to raise an event when virtual machine is either disconnected or removed. The default is unselected.
Event severity when virtual machine is either disconnected or removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which virtual machine is either disconnected or removed. The default is 15.
Additional Settings	
Event Details	
Event detail format	Select either **HTML Table** or **Plain Text** as the format for event detail. The default is HTML Table.
Monitor VMware Tools Status	
Event Notification	
Raise event when VMware Tools is outdated?	Select **Yes** to raise an event when a virtual machine is running an outdated version of VMware Tools. The default is Yes.

Parameter	How to Set It
Event severity when VMware Tools outdated	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a virtual machine is running an outdated version of VMware Tools. The default is 15.
Raise event when VMware Tools has never been installed?	Select **Yes** to raise an event when VMware Tools has never been installed on a virtual machine. The default is Yes.
Event severity when VMware Tools has never been installed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which VMware Tools has never been installed on a virtual machine. The default is 15.
Raise event when VMware Tools is not running?	Select **Yes** to raise an event when VMware Tools is not running on a virtual machine. The default is Yes.
Event severity when VMware Tools not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which VMware Tools is not running on a virtual machine. The default is 15.
Data Collection	
Collect data for VMware Tools status?	Select **Yes** to collect VMware Tools status data for charts and reports. The default is unselected. **Note** If selected, the possible values are: • 0 = tools not installed • 1 = tools not running • 2 = tools version old • 3 = tools OK

VirtualCenter_RPT_VCConfiguration

Use this Knowledge Script to generate a report about the configuration of each VMware host and its virtual machines for the selected vCenter server. It also includes details of the number of hosts configured per vCenter server.

If you do not discover all of the "object details," for example, in the Knowledge Script parameters, you unchecked the Discover X option, then you should run the Configuration Knowledge Script.

Each host report shows the following information:

- Type
- Version
- Build
- Number of CPUs
- CPU Speed
- Memory (in megabytes)
- Table of disks and their sizes (in megabytes)
- Table of virtual machines and their operating system

For each virtual machine, the report shows the following information:

- Host computer
- Guest operating system
- VM location
- Number of CPUs
- Memory (in megabytes)
- Table of hard disks, their type, and their size (in megabytes)
- Table of CD drives and their type
- Table of network interface cards, their type, emulation and MAC address

Resource Object

Report agent

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select computer	Select the computers you want to include in your report. Filter by view, computer or server group.

Parameter	How to Set It
Report Settings	
Include parameter table?	Select **Yes** to include a table of the parameter settings for your report. The default is Yes.
Select output folder	Click **Browse (...)** to define the file name for the report and to specify a default folder for the report. The default folder name is VMware.
Add job ID to output folder name?	Select **Yes** to add the job ID to the report's output folder name. The default is unselected. Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click **Browse [...]** to select report properties.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of your report, making each title unique. The time stamp includes the date and time the report was generated. The default is unselected. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event if the report is successfully generated. The default is Yes.
Event severity level when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35.
Event severity level when report contains no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25.
Event severity level when report failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation failed. The default is 5.

VirtualCenter_RPT_VCCPUUsage

Use this Knowledge Script to compare the CPU usage of a number of VMware hosts, and also to compare the CPU usage of their virtual machines.

This report uses the CPU usage data collected by the following Knowledge Scripts for the specified period:

- HostCPUUsage
- HostMemoryUsage
- HostDiskIO
- HostNetworkIO
- VmCPUusage
- VmMemoryUsage
- VmDiskIO
- VmNetworkIO

Prerequisite

Before generating reports, run the following Knowledge Scripts with the *Collect CPU data* option enabled:

- HostCPUUsage
- HostMemoryUsage
- HostDiskIO
- HostNetworkIO
- VmCPUusage
- VmMemoryUsage
- VmDiskIO
- VmNetworkIO

Resource Object

Report agent

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select computers	Select the computers you want to include in your report. Filter by view, computer or server group.

Parameter	How to Set It
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending in 24 hours.
Report Settings	
Include parameter table?	Select **Yes** to include a table of the parameter settings for your report. The default is Yes.
Select output folder	Click **Browse (...)** to define the file name for the report and to specify a default folder for the report. The default folder name is VMware.
Add job ID to output folder name?	Select **Yes** to add the job ID to the report's output folder name. The default is unselected. Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click **Browse [...]** to select report properties.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of your report, making each title unique. The time stamp includes the date and time the report was generated. The default is unselected. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Chart Parameters	
Maximum number of points on x axis	Specify the maximum number of data points to display on the x axis for a specific duration. If the amount of reported data points exceeds this number, separate graphs will be generated. The default is 50 data points.
Select chart style	Click **Browse [...]** to select the graphic properties for the charts in your report. The default is Line.
One chart per host or virtual machine?	By default, all host data is plotted on one graph, as is all virtual machine data for a given host computer. Enable this option to allow separate graphs for each host and each virtual machine. The default is unselected.
Horizontal size of charts in pixels	Set the horizontal size of generated charts in a range of pixels 400 to 1200. The default is 600 pixels.
Vertical size of charts in pixels	Set the vertical size of generated charts in a range of pixels from 260 to 800. The default is 400 pixels.
Select aggregate function	If a graph is to show fewer x-axis points than have been collected, select the way in which the data will be reduced with the function **AVG** (average), **MAX** or **MIN**. For example, if 1000 points were collected, but only 50 are to be shown on the graph, an average (or max/min.) will be calculated every 20 points. The default function is AVG.
Maximum number of x-axis data points	Specify the maximum total number of x-axis points to be reported for a chart. The default is 30.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event if the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35.

Parameter	How to Set It
Event severity when report contains no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25.
Event severity when report failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation failed. The default is 5.

VirtualCenter_RPT_VCHostDataStoreUsage

Use this Knowledge Script to compare host datastore usage in terms of free space available in megabytes and percentage of disk used. This report uses the datastore information collected by the HostDataStoreUsage Knowledge Script.

Prerequisite

Before generating reports, run the HostDataStoreUsage Knowledge Scripts with the *Collect free space and percentage used data* option enabled.

Resource Object

Report agent

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select computer	Select the computers you want to include in your report. Filter by view, computer or server group.
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending in 24 hours.
Report Settings	
Include parameter table?	Select **Yes** to include a table of the parameter settings for your report. The default is Yes.
Select output folder	Click **Browse (...)** to define the file name for the report and to specify a default folder for the report. The default folder name is VMware.
Add job ID to output folder name?	Select **Yes** to add the job ID to the report's output folder name. The default is unselected. Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click **Browse [...]** to select report properties.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of your report, making each title unique. The time stamp includes the date and time the report was generated. The default is unselected. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Chart Parameters	

Parameter	How to Set It
Maximum number of points on x axis	Specify the maximum number of data points to display on the x axis for a specific duration. If the amount of reported data points exceeds this number, separate graphs will be generated. The default is 50 data points.
Select chart style	Click **Browse [...]** to select the graphic properties for the charts in your report. The default is Line.
One chart per host?	By default, all host data is plotted on one graph. Select Yes to allow separate graphs for each host. The default is unselected.
Horizontal size of charts in pixels	Set the horizontal size of generated charts in a range of pixels 400 to 1200. The default is 600 pixels.
Vertical size of charts in pixels	Set the vertical size of generated charts in a range of pixels from 260 to 800. The default is 400 pixels.
Select aggregate function	If a graph is to show fewer x-axis points than have been collected, select the way in which the data will be reduced with the function **AVG** (average), **MAX** or **MIN**. For example, if 1000 points were collected, but only 50 are to be shown on the graph, an average (or max/min.) will be calculated every 20 points. The default function is AVG.
Maximum number of x-axis data points	Specify the maximum total number of x-axis points to be reported for a chart. The default is 30.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event if the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35.
Event severity when report contains no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25.
Event severity when report failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation failed. The default is 5.

VirtualCenter_RPT_VCMemoryUsage

Use this Knowledge Script to compare the memory usage of VMware hosts, and also to compare the memory usage of their virtual machines. This report uses the memory usage data collected by the HostMemoryUsage Knowledge Script.

Prerequisite

Before generating reports, run the HostMemoryUsage Knowledge Script with the data collection parameters set to Yes.

Resource Object

Report agent

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select computer	Select the computers you want to include in your report. Filter by view, computer or server group.
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending in 24 hours.
Report Settings	
Include parameter table?	Select **Yes** to include a table of the parameter settings for your report. The default is Yes.
Select output folder	Click **Browse (...)** to define the file name for the report and to specify a default folder for the report. The default folder name is VMware.
Add job ID to output folder name?	Select **Yes** to add the job ID to the report's output folder name. The default is unselected. Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click **Browse [...]** to select report properties.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of your report, making each title unique. The time stamp includes the date and time the report was generated. The default is unselected. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Chart Parameters	

Parameter	How to Set It
Maximum number of points on x axis	Specify the maximum number of data points to display on the x axis for a specific duration. If the amount of reported data points exceeds this number, separate graphs will be generated. The default is 50 data points.
Select chart style	Click **Browse [...]** to select the graphic properties for the charts in your report. The default is Line.
One chart per host or virtual machine?	By default, all host data is plotted on one graph, as is all virtual machine data for a given host computer. Enable this option to allow separate graphs for each host and each virtual machine. The default is unselected.
Horizontal size of charts in pixels	Set the horizontal size of generated charts in a range of pixels 400 to 1200. The default is 600 pixels.
Vertical size of charts in pixels	Set the vertical size of generated charts in a range of pixels from 260 to 800. The default is 400 pixels.
Select aggregate function	If a graph is to show fewer x-axis points than have been collected, select the way in which the data will be reduced with the function **AVG** (average), **MAX** or **MIN**. For example, if 1000 points were collected, but only 50 are to be shown on the graph, an average (or max/min.) will be calculated every 20 points. The default function is AVG.
Maximum number of x-axis data points	Specify the maximum total number of x-axis points to be reported for a chart. The default is 30.
Event Notification	
Raise event when report succeeds?	Select **Yes** to raise an event if the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35.
Event severity when report contains no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25.
Event severity when report fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation failed. The default is 5.

VirtualCenter_RPT_VCNetworkIO

Use this Knowledge Script to compare network reads/writes of VMware hosts, and to compare the network reads/writes of their virtual machines.

Resource Object

Report agent

Default Schedule

By default, this script runs **once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Data Source	
Select computer	Select the computers you want to include in your report. Filter by view, computer or server group.
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending in 24 hours.
Report Settings	
Include parameter table?	Select **Yes** to include a table of the parameter settings for your report. The default is Yes.
Select output folder	Click **Browse (...)** to define the file name for the report and to specify a default folder for the report. The default folder name is VMware.
Add job ID to output folder name?	Select **Yes** to add the job ID to the report's output folder name. The default is unselected. Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click **Browse [...]** to select report properties.
Add time stamp to title?	Select **Yes** to append a time stamp to the title of your report, making each title unique. The time stamp includes the date and time the report was generated. The default is unselected. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
Chart Parameters	**Chart Parameters**
Maximum number of points on x axis	Specify the maximum number of data points to display on the x axis for a specific duration. If the amount of reported data points exceeds this number, separate graphs will be generated. The default is 50 data points.
Select chart style	Click **Browse [...]** to select the graphic properties for the charts in your report. The default is Line.
One chart per host or virtual machine?	By default, all host data is plotted on one graph, as is all virtual machine data for a given host computer. Enable this option to allow separate graphs for each host and each virtual machine.

Parameter	How to Set It
Horizontal size of charts in pixels	Set the horizontal size of generated charts in a range of pixels 400 to 1200. The default is 600 pixels.
Vertical size of charts in pixels	Set the vertical size of generated charts in a range of pixels from 260 to 800. The default is 400 pixels.
Select aggregate function	If a graph is to show fewer x-axis points than have been collected, select the way in which the data will be reduced with the function **AVG** (average), **MAX** or **MIN**. For example, if 1000 points were collected, but only 50 are to be shown on the graph, an average (or max/min.) will be calculated every 20 points. The default function is AVG.
Maximum number of x-axis data points	Maximum total number of x-axis points to be reported for a chart. The default is 50.
Event Notification	
Raise event when report succeeds?	Select Yes to raise an event if the report is successfully generated. The default is Yes.
Event severity when report succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report is generated successfully. The default is 35.
Event severity when report contains no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a generated report contains no data. The default is 25.
Event severity when report failed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which report generation failed. The default is 5.

Recommended Knowledge Script Groups

You can find the VirtualCenter Knowledge Script Groups (KSGs) on the RECOMMENDED tab of the Knowledge Script pane of the Operator Console.

All the scripts in the KSGs have their parameters set to recommended values. To run all of the recommended scripts in a KSG at one time, click the RECOMMENDED tab, and then run the KSG on a VirtualCenter resource.

Run the KSG from the Master view, not the VirtualCenter view. In order to use the Discovery_VMware Knowledge Script in a monitoring policy, the view must include root objects, which are not visible in the VirtualCenter view.

The VirtualCenter KSGs enable a "best practices" usage of AppManager for monitoring your VirtualCenter environment. You can use these KSGs with AppManager monitoring policies. A monitoring policy, which lets you efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView pane. For more information, see "About Policy-Based Monitoring" in the AppManager Help.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the VirtualCenter tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the VirtualCenter tab are not affected.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the VirtualCenter KSG and want to restore it to its original form, you can reinstall AppManager for VMware on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\VirtualCenter` directory.

ClusterMonitor Recommended Knowledge Script Group

The following Knowledge Scripts in the AppManager for VMware module are members of the ClusterMonitor recommended KSG.

- ClusterCPUusage
- ClusterMemUsage
- ClusterStatus

HostMonitor Recommended Knowledge Script Group

The following Knowledge Scripts in the AppManager for VMware module are members of the HostMonitor recommended KSG.

- DatastoreUsage
- HostConnected
- HostCPUUsage
- HostDiskIO
- HostDiskTotalLatency
- HostMemoryUsage
- HostNetworkIO

ResourcePoolMonitor Recommended Knowledge Script Group

The following Knowledge Scripts in the AppManager for VMware module are members of the ResourcePoolMonitor recommended KSG.

- ResourcePoolCPUusage
- ResourcePoolMemUsage
- ResourcePoolStatus

VirtualCenterMonitor Recommended Knowledge Script Group

The following Knowledge Scripts in the AppManager for VMware module are members of the VirtualCenterMonitor recommended KSG.

- HostConnected
- HostCPUUsage
- HostMemoryUsage
- VmConnected
- VmCPUusage
- VmMemoryUsage

VirtualMachineMonitor Recommended Knowledge Script Group

The following Knowledge Scripts in the AppManager for VMware module are members of the VirtualMachineMonitor recommended KSG.

- VmCPUusage
- VmDiskIO
- VmDiskUsage
- VmMemoryUsage
- VmNetworkIO
- VmToolsStatus

Chapter 70
VoIPQuality Knowledge Scripts

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
CallPerf_G711a	Runs a VoIP test between Performance Endpoints for the G.711a codec.
CallPerf_G711u	Runs a VoIP test between Performance Endpoints for the G.711u codec.
CallPerf_G723.1-ACELP	Runs a VoIP test between Performance Endpoints for the G.723.1-ACELP codec.
CallPerf_G723.1-MPMLQ	Runs a VoIP test between Performance Endpoints for the G.723.1-MPMLQ codec.
CallPerf_G726	Runs a VoIP test between Performance Endpoints for the G.726 codec.
CallPerf_G729	Runs a VoIP test between Performance Endpoints for the G.729 codec.
CallPerf_G729A	Runs a VoIP test between Performance Endpoints for the G.729 Annex A codec.
CiscoSAA_G711a	Runs a VoIP test between Cisco SAA-enabled routers for the G.711a codec.
CiscoSAA_G711u	Runs a VoIP test between Cisco SAA-enabled routers for the G.711u codec.
CiscoSAA_G723.1-ACELP	Runs a VoIP test between Cisco SAA-enabled routers for the G.723.1-ACELP codec.
CiscoSAA_G723.1-MPMLQ	Runs a VoIP test between Cisco SAA-enabled routers for the G.723.1-MPMLQ codec.
CiscoSAA_G726	Runs a VoIP test between Cisco SAA-enabled routers for the G.726 codec.
CiscoSAA_G729	Runs a VoIP test between Cisco SAA-enabled routers for the G.729 codec.
CiscoSAA_G729A	Runs a VoIP test between Cisco SAA-enabled routers for the G.729 Annex A codec.
Report_Configuration	Summarizes VoIP Quality configuration information and summary information about which talkers are talking to which listeners for selected computers.
Report_GroupSummary	Summarizes group-to-group comparisons for VoIP Quality data streams.
Report_MOSAvailMatrix	Summarizes the average MOS and availability for valid talker-listener pairs.
Report_MOSSummary	Summarizes group-to-group comparisons for MOS breakdown.
Report_RvalueSummary	Summarizes group-to-group comparisons for R-value breakdown.
Report_TimeDetail	Summarizes time series charts for selected groups.
Report_VoIPQualitySummary	Summarizes VoIP quality statistics: MOS, delay, jitter, and packet loss.

CallPerf_G711a

Use this Knowledge Script to run a VoIP test between Performance Endpoints using the G.711a codec, which uses the A-law for companding, a popular standard in Europe. This script raises an event if a metric exceeds or falls below a threshold and generates data streams for network delay, MOS, R-value, delay, jitter, jitter buffer loss, and lost data.

Understanding Packet Loss Concealment

Packet loss concealment (PLC) is enabled by default in the G.711u and G.711a codecs. PLC describes a number of techniques for minimizing or masking the effects of data loss during a VoIP conversation. When PLC is enabled, the adverse affects of data loss are not as severe. AppManager calculates the call quality, factoring in the behavior of PLC, which is enabled by default in the CallPerf_G711a and CallPerf_G711u Knowledge Scripts.

In the following table, *packetization delay* refers to the delay these codecs introduce as they convert a signal from analog to digital; this delay is included in the MOS estimate, as is the *jitter buffer delay*, the delay introduced by the effects of buffering to reduce interarrival delay variations.

Codec	Default Data Rate	Default Datagram Size	Packetization Delay	Default Jitter Buffer Delay	Theoretical Maximum MOS
G.711u G.711a	64 kbps	20 ms	1.0 ms	2 datagrams (40 ms)	4.40
G.726	32kbps	20 ms	1.25 ms	2 datagrams (40 ms)	4.22
G.729 G.729A	8 kbps	20 ms	35.0 ms	2 datagrams (40 ms)	4.07
G.723.1-MPMLQ	6.3 kbps	30 ms	67.5 ms	3 datagrams (60 ms)	3.87
G.723.1-ACELP	5.3 kbps	30 ms	67.5 ms	3 datagrams (60 ms)	3.69

Resource Objects

Call Perf object

Call Perf proxy object

When you run this script on an agent computer that acts as proxy for multiple remote computers, AppManager creates only one job that drives the tests for all talkers on that computer. These tests run simultaneously. Running multiple tests at one time can take an undesirable toll on your bandwidth resources. Use the Objects tab on the Knowledge Script Properties dialog box to include or exclude remote resources from the tests.

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Select listener(s)	Select the listener computers from the Select Desired Computers dialog box.
Collect data?	Select **Yes** to collect data about MOS, R-value, delay, jitter, jitter buffer loss, and lost data for charts and graphs. The default is Yes.
Collect network delay data?	Select **Yes** to collect data about network delay for charts and graphs. The default is unselected.
Configuration Settings	
Test duration	Specify the duration of a test event in seconds, between one and 300. The default is 60 seconds.
Service Quality	Select a DiffServ (Differentiated Services) codepoint for classifying the bits in the IP header: • **None**. Default setting. No special treatment is given to packets. • **EF0-101000**. Deprecated Expedited Flow codepoint in use by most phones. Equivalent to the TOS "CRITIC/ECP" setting reserved for voice. • **EF-101110**. Expedited Forwarding per-hop behavior (PHB) codepoint, represents the highest-priority service. • **AF-011000**. Deprecated Assured Flow per-hop behavior (PHB) codepoint, represents a medium-quality service. Equivalent to the TOS "flash" setting. • **AF11-001010** (Assured Forwarding, Class 1, low drop precedence) • **AF12 - 001100** (Assured Forwarding, Class 1, medium drop precedence) • **AF13-001110** (Assured Forwarding, Class 1, high drop precedence) • **AF2 -010010** (Assured Forwarding, Class 2, low drop precedence) • **AF22-010100** (Assured Forwarding, Class 2, medium drop precedence) • **AF23-010110** (Assured Forwarding, Class 2, high drop precedence) • **AF31 011010** (Assured Forwarding, Class 3, low drop precedence) • **AF32-011100** (Assured Forwarding, Class 3, medium drop precedence) • **AF33-011110** (Assured Forwarding, Class 3, high drop precedence) • **AF4 -100010** (Assured Forwarding, Class 4, low drop precedence) • **AF42-100100** (Assured Forwarding, Class 4, medium drop precedence) • **AF43-100110** (Assured Forwarding, Class 4, high drop precedence) • **802.1p-011** (For medium-priority traffic, often used for call setup packets) • **802.1p-101** (For high-priority traffic, recommended for VoIP data packets)
Voice activity rate	Specify a voice activity rate percentage. For example, enter 50 to indicate that data is being sent during 50% of a call's duration. The default is 50%.
Delay between voice datagrams	Specify a delay, in milliseconds, between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Use silence suppression?	Select **Yes** to enable silence suppression, which means that no data is sent during periods of “call silence” (i.e. when no one is talking). The default is unselected.

Parameter	How To Set It
Enable packet loss concealment?	Select **Yes** to enable packet loss concealment (PLC). PLC is a technique for minimizing or masking the effects of data loss. When PLC is enabled, AppManager assumes that the quality of a conversation would be improved, but the improvement is factored into a MOS calculation **only** if data is lost. The default is Yes.
Advanced Configuration Settings	
Absolute jitter buffer size	Specify the size of the absolute jitter buffer in milliseconds. The jitter buffer size is a critical component of the MOS calculation. For example, a jitter buffer of 43 ms could hold two 20-ms datagram packets and allow for three extra milliseconds of variability. The default is 40 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Event Notification	
Raise event if test fails?	Select **Yes** to raise an event if the VoIP test does not complete successfully. The default is Yes.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VoIP test does not complete successfully. The default is 5.
Raise event if MOS/R-value falls below threshold	Select **Yes** to raise an event if the MOS score or R-value falls below the threshold that you set. The default is Yes.
VoIP quality metric for event	Select the VoIP quality metric you want to use for the VoIP test. The default is MOS. • **MOS**. The Mean Opinion Score (MOS) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. The MOS is calculated based on measured items plus jitter buffer size. The jitter buffer size is constant based on the codec/script. Only one jitter buffer size is specified and used throughout the test. • **R-value**. A single score that is derived from delays and equipment impairment factors. An R-value can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor).
Threshold - Minimum MOS	Specify the minimum Mean Opinion Score (MOS) that must be reached to prevent an event from being raised. The default is 3.60.
Threshold - Minimum R-value	Specify the minimum acceptable R-value that must be reached to prevent an event from being raised. The default is 70.
Event severity when VoIP quality falls below threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which MOS or R-value falls below the threshold that you set. The default is 5.
Raise event if delay exceeds threshold?	Select **Yes** to raise an event if delay exceeds the threshold that you set. The default is Yes.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets. The default is 400 ms.

Parameter	How To Set It
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold that you set. The default is 15.
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if jitter exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets. The default is 60 ms.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold that you set. The default is 15.
Raise event if jitter buffer loss exceeds threshold?	Select **Yes** to raise an event if jitter buffer loss exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter buffer loss	Specify the maximum percentage of jitter buffer loss that can occur before an event is raised. The default is 1.0%. Jitter buffer loss is the amount of data that is lost when jitter exceeds that which the jitter buffer can hold. Jitter buffer loss affects call clarity, which affects the overall MOS score.
Event severity when jitter buffer loss exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter buffer loss exceeds the threshold that you set. The default is 15.
Raise event if lost data exceeds threshold?	Select **Yes** to raise an event if lost data exceeds the threshold that you set. The default is Yes.
Threshold - Maximum lost data	Specify the maximum percentage of lost data that can occur before an event is raised. The default is 1.0%. To calculate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold that you set. The default is 15.

CallPerf_G711u

Use this Knowledge Script to run a VoIP test between Performance Endpoints using the G.711u codec, which uses the u-law for companding, the most frequently used method in the USA. This script raises an event if a metric exceeds or falls below a threshold and generates data streams for network delay, MOS, R-value, delay, jitter, jitter buffer loss, and lost data.

Understanding Packet Loss Concealment

Packet loss concealment (PLC) is enabled by default in the G.711u and G.711a codecs. PLC describes a number of techniques for minimizing or masking the effects of data loss during a VoIP conversation. When PLC is enabled, the adverse affects of data loss are not as severe. AppManager calculates the call quality, factoring in the behavior of PLC, which is enabled by default in the CallPerf_G711a and CallPerf_G711u Knowledge Scripts.

In the following table, *packetization delay* refers to the delay these codecs introduce as they convert a signal from analog to digital; this delay is included in the MOS estimate, as is the *jitter buffer delay*, the delay introduced by the effects of buffering to reduce interarrival delay variations.

Codec	Default Data Rate	Default Datagram Size	Packetization Delay	Default Jitter Buffer Delay	Theoretical Maximum MOS
G.711u G.711a	64 kbps	20 ms	1.0 ms	2 datagrams (40 ms)	4.40
G.726	32kbps	20 ms	1.25 ms	2 datagrams (40 ms)	4.22
G.729 G.729A	8 kbps	20 ms	35.0 ms	2 datagrams (40 ms)	4.07
G.723.1-MPMLQ	6.3 kbps	30 ms	67.5 ms	3 datagrams (60 ms)	3.87
G.723.1-ACELP	5.3 kbps	30 ms	67.5 ms	3 datagrams (60 ms)	3.69

Resource Objects

Call Perf object

Call Perf proxy object

When you run this script on an agent computer that acts as proxy for multiple remote computers, AppManager creates only one job that drives the tests for all talkers on that computer. These tests run simultaneously. Running multiple tests at one time can take an undesirable toll on your bandwidth resources. Use the Objects tab on the Knowledge Script Properties dialog box to include or exclude remote resources from the tests.

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Select listener(s)	Select the listener computers from the Select Desired Computers dialog box.
Collect data?	Select **Yes** to collect data about MOS, R-value, delay, jitter, jitter buffer loss, and lost data for charts and graphs. The default is Yes.
Collect network delay data?	Select **Yes** to collect data about network delay for charts and graphs. The default is unselected.
Configuration Settings	
Test duration	Specify the duration of a test event in seconds, between one and 300. The default is 60 seconds.
Service Quality	Select a DiffServ (Differentiated Services) codepoint for classifying the bits in the IP header: • **None**. Default setting. No special treatment is given to packets. • **EF0-101000**. Deprecated Expedited Flow codepoint in use by most phones. Equivalent to the TOS "CRITIC/ECP" setting reserved for voice. • **EF-101110**. Expedited Forwarding per-hop behavior (PHB) codepoint, represents the highest-priority service. • **AF-011000**. Deprecated Assured Flow per-hop behavior (PHB) codepoint, represents a medium-quality service. Equivalent to the TOS "flash" setting. • **AF11-001010** (Assured Forwarding, Class 1, low drop precedence) • **AF12 - 001100** (Assured Forwarding, Class 1, medium drop precedence) • **AF13-001110** (Assured Forwarding, Class 1, high drop precedence) • **AF2 -010010** (Assured Forwarding, Class 2, low drop precedence) • **AF22-010100** (Assured Forwarding, Class 2, medium drop precedence) • **AF23-010110** (Assured Forwarding, Class 2, high drop precedence) • **AF31 011010** (Assured Forwarding, Class 3, low drop precedence) • **AF32-011100** (Assured Forwarding, Class 3, medium drop precedence) • **AF33-011110** (Assured Forwarding, Class 3, high drop precedence) • **AF4 -100010** (Assured Forwarding, Class 4, low drop precedence) • **AF42-100100** (Assured Forwarding, Class 4, medium drop precedence) • **AF43-100110** (Assured Forwarding, Class 4, high drop precedence) • **802.1p-011** (For medium-priority traffic, often used for call setup packets) • **802.1p-101** (For high-priority traffic, recommended for VoIP data packets)
Voice activity rate	Specify a voice activity rate percentage. For example, enter 50 to indicate that data is being sent during 50% of a call's duration. The default is 50%.
Delay between voice datagrams	Specify a delay, in milliseconds, between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Use silence suppression?	Select **Yes** to enable silence suppression, which means that no data is sent during periods of “call silence” (i.e. when no one is talking). The default is unselected.

Parameter	How To Set It
Enable packet loss concealment?	Select **Yes** to enable packet loss concealment (PLC). PLC is a technique for minimizing or masking the effects of data loss. When PLC is enabled, AppManager assumes that the quality of a conversation would be improved, but the improvement is factored into a MOS calculation **only** if data is lost. The default is Yes.
Advanced Configuration Settings	
Absolute jitter buffer size	Specify the size of the absolute jitter buffer in milliseconds. The jitter buffer size is a critical component of the MOS calculation. For example, a jitter buffer of 43 ms could hold two 20-ms datagram packets and allow for three extra milliseconds of variability. The default is 40 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Event Notification	
Raise event if test fails?	Select **Yes** to raise an event if the VoIP test does not complete successfully. The default is Yes.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VoIP test does not complete successfully. The default is 5.
Raise event if MOS/R-value falls below threshold	Select **Yes** to raise an event if the MOS score or R-value falls below the threshold that you set. The default is Yes.
VoIP quality metric for event	Select the VoIP quality metric you want to use for the VoIP test. The default is MOS. • **MOS**. The Mean Opinion Score (MOS) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. The MOS is calculated based on measured items plus jitter buffer size. The jitter buffer size is constant based on the codec/script. Only one jitter buffer size is specified and used throughout the test. • **R-value**. A single score that is derived from delays and equipment impairment factors. An R-value can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor).
Threshold - Minimum MOS	Specify the minimum Mean Opinion Score (MOS) that must be reached to prevent an event from being raised. The default is 3.60.
Threshold - Minimum R-value	Specify the minimum acceptable R-value that must be reached to prevent an event from being raised. The default is 70.
Event severity when VoIP quality falls below threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which MOS or R-value falls below the threshold that you set. The default is 5.
Raise event if delay exceeds threshold?	Select **Yes** to raise an event if delay exceeds the threshold that you set. The default is Yes.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets. The default is 400 ms.

Parameter	How To Set It
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold that you set. The default is 15.
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if jitter exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets. The default is 60 ms.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold that you set. The default is 15.
Raise event if jitter buffer loss exceeds threshold?	Select **Yes** to raise an event if jitter buffer loss exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter buffer loss	Specify the maximum percentage of jitter buffer loss that can occur before an event is raised. The default is 1.0%. Jitter buffer loss is the amount of data that is lost when jitter exceeds that which the jitter buffer can hold. Jitter buffer loss affects call clarity, which affects the overall MOS score.
Event severity when jitter buffer loss exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter buffer loss exceeds the threshold that you set. The default is 15.
Raise event if lost data exceeds threshold?	Select **Yes** to raise an event if lost data exceeds the threshold that you set. The default is Yes.
Threshold - Maximum lost data	Specify the maximum percentage of lost data that can occur before an event is raised. The default is 1.0%. To calculate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold that you set. The default is 15.

CallPerf_G723.1-ACELP

Use this Knowledge Script to run a VoIP test between Performance Endpoints using the G.723.1-ACELP codec, which uses the conjugate structure algebraic code excited linear predictive compression (ACELP) algorithm. This script raises an event if a metric exceeds or falls below a threshold and generates data streams for network delay, MOS, R-value, delay, jitter, jitter buffer loss, and lost data.

Resource Objects

Call Perf object

Call Perf proxy object

When you run this script on an agent computer that acts as proxy for multiple remote computers, AppManager creates only one job that drives the tests for all talkers on that computer. These tests run simultaneously. Running multiple tests at one time can take an undesirable toll on your bandwidth resources. Use the Objects tab on the Knowledge Script Properties dialog box to include or exclude remote resources from the tests.

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Select listener(s)	Select the listener computers from the Select Desired Computers dialog box.
Collect data?	Select **Yes** to collect data about MOS, R-value, delay, jitter, jitter buffer loss, and lost data for charts and graphs. The default is Yes.
Collect network delay data?	Select **Yes** to collect data about network delay for charts and graphs. The default is unselected.
Configuration Settings	
Test duration	Specify the duration of a test event in seconds, between one and 300. The default is 60 seconds.

Parameter	How To Set It
Service Quality	Select a DiffServ (Differentiated Services) codepoint for classifying the bits in the IP header: • **None**. Default setting. No special treatment is given to packets. • **EF0-101000**. Deprecated Expedited Flow codepoint in use by most phones. Equivalent to the TOS "CRITIC/ECP" setting reserved for voice. • **EF-101110**. Expedited Forwarding per-hop behavior (PHB) codepoint, represents the highest-priority service. • **AF-011000**. Deprecated Assured Flow per-hop behavior (PHB) codepoint, represents a medium-quality service. Equivalent to the TOS "flash" setting. • **AF11-001010** (Assured Forwarding, Class 1, low drop precedence) • **AF12 - 001100** (Assured Forwarding, Class 1, medium drop precedence) • **AF13-001110** (Assured Forwarding, Class 1, high drop precedence) • **AF2 -010010** (Assured Forwarding, Class 2, low drop precedence) • **AF22-010100** (Assured Forwarding, Class 2, medium drop precedence) • **AF23-010110** (Assured Forwarding, Class 2, high drop precedence) • **AF31 011010** (Assured Forwarding, Class 3, low drop precedence) • **AF32-011100** (Assured Forwarding, Class 3, medium drop precedence) • **AF33-011110** (Assured Forwarding, Class 3, high drop precedence) • **AF4 -100010** (Assured Forwarding, Class 4, low drop precedence) • **AF42-100100** (Assured Forwarding, Class 4, medium drop precedence) • **AF43-100110** (Assured Forwarding, Class 4, high drop precedence) • **802.1p-011** (For medium-priority traffic, often used for call setup packets) • **802.1p-101** (For high-priority traffic, recommended for VoIP data packets)
Voice activity rate	Specify a voice activity rate percentage. For example, enter 50 to indicate that data is being sent during 50% of a call's duration. The default is 50%.
Delay between voice datagrams	Specify a delay, in milliseconds, between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Use silence suppression?	Select **Yes** to enable silence suppression, which means that no data is sent during periods of “call silence” (i.e. when no one is talking). The default is unselected.
Advanced Configuration Settings	
Absolute jitter buffer size	Specify the size of the absolute jitter buffer in milliseconds. The jitter buffer size is a critical component of the MOS calculation. For example, a jitter buffer of 43 ms could hold two 20-ms datagram packets and allow for three extra milliseconds of variability. The default is 40 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Event Notification	

Parameter	How To Set It
Raise event if test fails?	Select **Yes** to raise an event if the VoIP test does not complete successfully. The default is Yes.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VoIP test does not complete successfully. The default is 5.
Raise event if MOS/R-value falls below threshold	Select **Yes** to raise an event if the MOS score or R-value falls below the threshold that you set. The default is Yes.
VoIP quality metric for event	Select the VoIP quality metric you want to use for the VoIP test. The default is MOS. • **MOS**. The Mean Opinion Score (MOS) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. The MOS is calculated based on measured items plus jitter buffer size. The jitter buffer size is constant based on the codec/script. Only one jitter buffer size is specified and used throughout the test. • **R-value**. A single score that is derived from delays and equipment impairment factors. An R-value can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor).
Threshold - Minimum MOS	Specify the minimum Mean Opinion Score (MOS) that must be reached to prevent an event from being raised. The default is 3.60.
Threshold - Minimum R-value	Specify the minimum acceptable R-value that must be reached to prevent an event from being raised. The default is 70.
Event severity when VoIP quality falls below threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which MOS or R-value falls below the threshold that you set. The default is 5.
Raise event if delay exceeds threshold?	Select **Yes** to raise an event if delay exceeds the threshold that you set. The default is Yes.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets. The default is 400 ms.
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold that you set. The default is 15.
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if jitter exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets. The default is 60 ms.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold that you set. The default is 15.
Raise event if jitter buffer loss exceeds threshold?	Select **Yes** to raise an event if jitter buffer loss exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter buffer loss	Specify the maximum percentage of jitter buffer loss that can occur before an event is raised. The default is 1.0%. Jitter buffer loss is the amount of data that is lost when jitter exceeds that which the jitter buffer can hold. Jitter buffer loss affects call clarity, which affects the overall MOS score.
Event severity when jitter buffer loss exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter buffer loss exceeds the threshold that you set. The default is 15.
Raise event if lost data exceeds threshold?	Select **Yes** to raise an event if lost data exceeds the threshold that you set. The default is Yes.

Parameter	How To Set It
Threshold - Maximum lost data	Specify the maximum percentage of lost data that can occur before an event is raised. The default is 1.0%. To calculate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold that you set. The default is 15.

CallPerf_G723.1-MPMLQ

Use this Knowledge Script to run a VoIP test between Performance Endpoints using the G.723.1-MPMLQ codec, which uses the multipulse maximum likelihood quantization (MPMLQ) compression algorithm. This script raises an event if a metric exceeds or falls below a threshold and generates data streams for network delay, MOS, R-value, delay, jitter, jitter buffer loss, and lost data.

Resource Objects

Call Perf object

Call Perf proxy object

When you run this script on an agent computer that acts as proxy for multiple remote computers, AppManager creates only one job that drives the tests for all talkers on that computer. These tests run simultaneously. Running multiple tests at one time can take an undesirable toll on your bandwidth resources. Use the Objects tab on the Knowledge Script Properties dialog box to include or exclude remote resources from the tests.

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Select listener(s)	Select the listener computers from the Select Desired Computers dialog box.
Collect data?	Select **Yes** to collect data about MOS, R-value, delay, jitter, jitter buffer loss, and lost data for charts and graphs. The default is Yes.
Collect network delay data?	Select **Yes** to collect data about network delay for charts and graphs. The default is unselected.
Configuration Settings	
Test duration	Specify the duration of a test event in seconds, between one and 300. The default is 60 seconds.

Parameter	How To Set It
Service Quality	Select a DiffServ (Differentiated Services) codepoint for classifying the bits in the IP header: • **None**. Default setting. No special treatment is given to packets. • **EF0-101000**. Deprecated Expedited Flow codepoint in use by most phones. Equivalent to the TOS "CRITIC/ECP" setting reserved for voice. • **EF-101110**. Expedited Forwarding per-hop behavior (PHB) codepoint, represents the highest-priority service. • **AF-011000**. Deprecated Assured Flow per-hop behavior (PHB) codepoint, represents a medium-quality service. Equivalent to the TOS "flash" setting. • **AF11-001010** (Assured Forwarding, Class 1, low drop precedence) • **AF12 - 001100** (Assured Forwarding, Class 1, medium drop precedence) • **AF13-001110** (Assured Forwarding, Class 1, high drop precedence) • **AF2 -010010** (Assured Forwarding, Class 2, low drop precedence) • **AF22-010100** (Assured Forwarding, Class 2, medium drop precedence) • **AF23-010110** (Assured Forwarding, Class 2, high drop precedence) • **AF31 011010** (Assured Forwarding, Class 3, low drop precedence) • **AF32-011100** (Assured Forwarding, Class 3, medium drop precedence) • **AF33-011110** (Assured Forwarding, Class 3, high drop precedence) • **AF4 -100010** (Assured Forwarding, Class 4, low drop precedence) • **AF42-100100** (Assured Forwarding, Class 4, medium drop precedence) • **AF43-100110** (Assured Forwarding, Class 4, high drop precedence) • **802.1p-011** (For medium-priority traffic, often used for call setup packets) • **802.1p-101** (For high-priority traffic, recommended for VoIP data packets)
Voice activity rate	Specify a voice activity rate percentage. For example, enter 50 to indicate that data is being sent during 50% of a call's duration. The default is 50%.
Delay between voice datagrams	Specify a delay, in milliseconds, between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Use silence suppression?	Select **Yes** to enable silence suppression, which means that no data is sent during periods of “call silence” (i.e. when no one is talking). The default is unselected.
Advanced Configuration Settings	
Absolute jitter buffer size	Specify the size of the absolute jitter buffer in milliseconds. The jitter buffer size is a critical component of the MOS calculation. For example, a jitter buffer of 43 ms could hold two 20-ms datagram packets and allow for three extra milliseconds of variability. The default is 40 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Event Notification	

Parameter	How To Set It
Raise event if test fails?	Select **Yes** to raise an event if the VoIP test does not complete successfully. The default is Yes.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VoIP test does not complete successfully. The default is 5.
Raise event if MOS/R-value falls below threshold	Select **Yes** to raise an event if the MOS score or R-value falls below the threshold that you set. The default is Yes.
VoIP quality metric for event	Select the VoIP quality metric you want to use for the VoIP test. The default is MOS. • **MOS**. The Mean Opinion Score (MOS) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. The MOS is calculated based on measured items plus jitter buffer size. The jitter buffer size is constant based on the codec/script. Only one jitter buffer size is specified and used throughout the test. • **R-value**. A single score that is derived from delays and equipment impairment factors. An R-value can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor).
Threshold - Minimum MOS	Specify the minimum Mean Opinion Score (MOS) that must be reached to prevent an event from being raised. The default is 3.60.
Threshold - Minimum R-value	Specify the minimum acceptable R-value that must be reached to prevent an event from being raised. The default is 70.
Event severity when VoIP quality falls below threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which MOS or R-value falls below the threshold that you set. The default is 5.
Raise event if delay exceeds threshold?	Select **Yes** to raise an event if delay exceeds the threshold that you set. The default is Yes.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets. The default is 400 ms.
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold that you set. The default is 15.
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if jitter exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets. The default is 60 ms.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold that you set. The default is 15.
Raise event if jitter buffer loss exceeds threshold?	Select **Yes** to raise an event if jitter buffer loss exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter buffer loss	Specify the maximum percentage of jitter buffer loss that can occur before an event is raised. The default is 1.0%. Jitter buffer loss is the amount of data that is lost when jitter exceeds that which the jitter buffer can hold. Jitter buffer loss affects call clarity, which affects the overall MOS score.
Event severity when jitter buffer loss exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter buffer loss exceeds the threshold that you set. The default is 15.
Raise event if lost data exceeds threshold?	Select **Yes** to raise an event if lost data exceeds the threshold that you set. The default is Yes.

Parameter	How To Set It
Threshold - Maximum lost data	Specify the maximum percentage of lost data that can occur before an event is raised. The default is 1.0%. To calculate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold that you set. The default is 15.

CallPerf_G726

Use this Knowledge Script to run a VoIP test between Performance Endpoints using the G.726 codec, a waveform coder that uses Adaptive Differential Pulse Code Modulation (ADPCM). ADPCM is a variation of pulse code modulation (PCM), which sends only the difference between two adjacent samples, producing a lower bit rate. This script raises an event if a metric exceeds or falls below a threshold and generates data streams for network delay, MOS, R-value, delay, jitter, jitter buffer loss, and lost data.

Resource Objects

Call Perf object

Call Perf proxy object

When you run this script on an agent computer that acts as proxy for multiple remote computers, AppManager creates only one job that drives the tests for all talkers on that computer. These tests run simultaneously. Running multiple tests at one time can take an undesirable toll on your bandwidth resources. Use the Objects tab on the Knowledge Script Properties dialog box to include or exclude remote resources from the tests.

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Select listener(s)	Select the listener computers from the Select Desired Computers dialog box.
Collect data?	Select **Yes** to collect data about MOS, R-value, delay, jitter, jitter buffer loss, and lost data for charts and graphs. The default is Yes.
Collect network delay data?	Select **Yes** to collect data about network delay for charts and graphs. The default is unselected.
Configuration Settings	
Test duration	Specify the duration of a test event in seconds, between one and 300. The default is 60 seconds.

Parameter	How To Set It
Service Quality	Select a DiffServ (Differentiated Services) codepoint for classifying the bits in the IP header: • **None**. Default setting. No special treatment is given to packets. • **EF0-101000**. Deprecated Expedited Flow codepoint in use by most phones. Equivalent to the TOS "CRITIC/ECP" setting reserved for voice. • **EF-101110**. Expedited Forwarding per-hop behavior (PHB) codepoint, represents the highest-priority service. • **AF-011000**. Deprecated Assured Flow per-hop behavior (PHB) codepoint, represents a medium-quality service. Equivalent to the TOS "flash" setting. • **AF11-001010** (Assured Forwarding, Class 1, low drop precedence) • **AF12 - 001100** (Assured Forwarding, Class 1, medium drop precedence) • **AF13-001110** (Assured Forwarding, Class 1, high drop precedence) • **AF2 -010010** (Assured Forwarding, Class 2, low drop precedence) • **AF22-010100** (Assured Forwarding, Class 2, medium drop precedence) • **AF23-010110** (Assured Forwarding, Class 2, high drop precedence) • **AF31 011010** (Assured Forwarding, Class 3, low drop precedence) • **AF32-011100** (Assured Forwarding, Class 3, medium drop precedence) • **AF33-011110** (Assured Forwarding, Class 3, high drop precedence) • **AF4 -100010** (Assured Forwarding, Class 4, low drop precedence) • **AF42-100100** (Assured Forwarding, Class 4, medium drop precedence) • **AF43-100110** (Assured Forwarding, Class 4, high drop precedence) • **802.1p-011** (For medium-priority traffic, often used for call setup packets) • **802.1p-101** (For high-priority traffic, recommended for VoIP data packets)
Voice activity rate	Specify a voice activity rate percentage. For example, enter 50 to indicate that data is being sent during 50% of a call's duration. The default is 50%.
Delay between voice datagrams	Specify a delay, in milliseconds, between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Use silence suppression?	Select **Yes** to enable silence suppression, which means that no data is sent during periods of “call silence” (i.e. when no one is talking). The default is unselected.
Advanced Configuration Settings	
Absolute jitter buffer size	Specify the size of the absolute jitter buffer in milliseconds. The jitter buffer size is a critical component of the MOS calculation. For example, a jitter buffer of 43 ms could hold two 20-ms datagram packets and allow for three extra milliseconds of variability. The default is 40 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Event Notification	

Parameter	How To Set It
Raise event if test fails?	Select **Yes** to raise an event if the VoIP test does not complete successfully. The default is Yes.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VoIP test does not complete successfully. The default is 5.
Raise event if MOS/R-value falls below threshold	Select **Yes** to raise an event if the MOS score or R-value falls below the threshold that you set. The default is Yes.
VoIP quality metric for event	Select the VoIP quality metric you want to use for the VoIP test. The default is MOS. • **MOS**. The Mean Opinion Score (MOS) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. The MOS is calculated based on measured items plus jitter buffer size. The jitter buffer size is constant based on the codec/script. Only one jitter buffer size is specified and used throughout the test. • **R-value**. A single score that is derived from delays and equipment impairment factors. An R-value can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor).
Threshold - Minimum MOS	Specify the minimum Mean Opinion Score (MOS) that must be reached to prevent an event from being raised. The default is 3.60.
Threshold - Minimum R-value	Specify the minimum acceptable R-value that must be reached to prevent an event from being raised. The default is 70.
Event severity when VoIP quality falls below threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which MOS or R-value falls below the threshold that you set. The default is 5.
Raise event if delay exceeds threshold?	Select **Yes** to raise an event if delay exceeds the threshold that you set. The default is Yes.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets. The default is 400 ms.
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold that you set. The default is 15.
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if jitter exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets. The default is 60 ms.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold that you set. The default is 15.
Raise event if jitter buffer loss exceeds threshold?	Select **Yes** to raise an event if jitter buffer loss exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter buffer loss	Specify the maximum percentage of jitter buffer loss that can occur before an event is raised. The default is 1.0%. Jitter buffer loss is the amount of data that is lost when jitter exceeds that which the jitter buffer can hold. Jitter buffer loss affects call clarity, which affects the overall MOS score.
Event severity when jitter buffer loss exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter buffer loss exceeds the threshold that you set. The default is 15.
Raise event if lost data exceeds threshold?	Select **Yes** to raise an event if lost data exceeds the threshold that you set. The default is Yes.

Parameter	How To Set It
Threshold - Maximum lost data	Specify the maximum percentage of lost data that can occur before an event is raised. The default is 1.0%. To calculate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold that you set. The default is 15.

CallPerf_G729

Use this Knowledge Script to run a VoIP test between Performance Endpoints using the G.729 codec, which offers compression with high quality. This script raises an event if a metric exceeds or falls below a threshold and generates data streams for network delay, MOS, R-value, delay, jitter, jitter buffer loss, and lost data.

Resource Objects

Call Perf object

Call Perf proxy object

When you run this script on an agent computer that acts as proxy for multiple remote computers, AppManager creates only one job that drives the tests for all talkers on that computer. These tests run simultaneously. Running multiple tests at one time can take an undesirable toll on your bandwidth resources. Use the Objects tab on the Knowledge Script Properties dialog box to include or exclude remote resources from the tests.

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Select listener(s)	Select the listener computers from the Select Desired Computers dialog box.
Collect data?	Select **Yes** to collect data about MOS, R-value, delay, jitter, jitter buffer loss, and lost data for charts and graphs. The default is Yes.
Collect network delay data?	Select **Yes** to collect data about network delay for charts and graphs. The default is unselected.
Configuration Settings	
Test duration	Specify the duration of a test event in seconds, between one and 300. The default is 60 seconds.

Parameter	How To Set It
Service Quality	Select a DiffServ (Differentiated Services) codepoint for classifying the bits in the IP header: • **None**. Default setting. No special treatment is given to packets. • **EF0-101000**. Deprecated Expedited Flow codepoint in use by most phones. Equivalent to the TOS "CRITIC/ECP" setting reserved for voice. • **EF-101110**. Expedited Forwarding per-hop behavior (PHB) codepoint, represents the highest-priority service. • **AF-011000**. Deprecated Assured Flow per-hop behavior (PHB) codepoint, represents a medium-quality service. Equivalent to the TOS "flash" setting. • **AF11-001010** (Assured Forwarding, Class 1, low drop precedence) • **AF12 - 001100** (Assured Forwarding, Class 1, medium drop precedence) • **AF13-001110** (Assured Forwarding, Class 1, high drop precedence) • **AF2 -010010** (Assured Forwarding, Class 2, low drop precedence) • **AF22-010100** (Assured Forwarding, Class 2, medium drop precedence) • **AF23-010110** (Assured Forwarding, Class 2, high drop precedence) • **AF31 011010** (Assured Forwarding, Class 3, low drop precedence) • **AF32-011100** (Assured Forwarding, Class 3, medium drop precedence) • **AF33-011110** (Assured Forwarding, Class 3, high drop precedence) • **AF4 -100010** (Assured Forwarding, Class 4, low drop precedence) • **AF42-100100** (Assured Forwarding, Class 4, medium drop precedence) • **AF43-100110** (Assured Forwarding, Class 4, high drop precedence) • **802.1p-011** (For medium-priority traffic, often used for call setup packets) • **802.1p-101** (For high-priority traffic, recommended for VoIP data packets)
Voice activity rate	Specify a voice activity rate percentage. For example, enter 50 to indicate that data is being sent during 50% of a call's duration. The default is 50%.
Delay between voice datagrams	Specify a delay, in milliseconds, between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Use silence suppression?	Select **Yes** to enable silence suppression, which means that no data is sent during periods of “call silence” (i.e. when no one is talking). The default is unselected.
Advanced Configuration Settings	
Absolute jitter buffer size	Specify the size of the absolute jitter buffer in milliseconds. The jitter buffer size is a critical component of the MOS calculation. For example, a jitter buffer of 43 ms could hold two 20-ms datagram packets and allow for three extra milliseconds of variability. The default is 40 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Event Notification	

Parameter	How To Set It
Raise event if test fails?	Select **Yes** to raise an event if the VoIP test does not complete successfully. The default is Yes.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VoIP test does not complete successfully. The default is 5.
Raise event if MOS/R-value falls below threshold	Select **Yes** to raise an event if the MOS score or R-value falls below the threshold that you set. The default is Yes.
VoIP quality metric for event	Select the VoIP quality metric you want to use for the VoIP test. The default is MOS. • **MOS**. The Mean Opinion Score (MOS) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. The MOS is calculated based on measured items plus jitter buffer size. The jitter buffer size is constant based on the codec/script. Only one jitter buffer size is specified and used throughout the test. • **R-value**. A single score that is derived from delays and equipment impairment factors. An R-value can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor).
Threshold - Minimum MOS	Specify the minimum Mean Opinion Score (MOS) that must be reached to prevent an event from being raised. The default is 3.60.
Threshold - Minimum R-value	Specify the minimum acceptable R-value that must be reached to prevent an event from being raised. The default is 70.
Event severity when VoIP quality falls below threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which MOS or R-value falls below the threshold that you set. The default is 5.
Raise event if delay exceeds threshold?	Select **Yes** to raise an event if delay exceeds the threshold that you set. The default is Yes.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets. The default is 400 ms.
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold that you set. The default is 15.
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if jitter exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets. The default is 60 ms.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold that you set. The default is 15.
Raise event if jitter buffer loss exceeds threshold?	Select **Yes** to raise an event if jitter buffer loss exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter buffer loss	Specify the maximum percentage of jitter buffer loss that can occur before an event is raised. The default is 1.0%. Jitter buffer loss is the amount of data that is lost when jitter exceeds that which the jitter buffer can hold. Jitter buffer loss affects call clarity, which affects the overall MOS score.
Event severity when jitter buffer loss exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter buffer loss exceeds the threshold that you set. The default is 15.
Raise event if lost data exceeds threshold?	Select **Yes** to raise an event if lost data exceeds the threshold that you set. The default is Yes.

Parameter	How To Set It
Threshold - Maximum lost data	Specify the maximum percentage of lost data that can occur before an event is raised. The default is 1.0%. To calculate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold that you set. The default is 15.

CallPerf_G729A

Use this Knowledge Script to run a VoIP test between Performance Endpoints using the G.729 Annex A codec, which offers compression with high quality. This script raises an event if a metric exceeds or falls below a threshold and generates data streams for network delay, MOS, R-value, delay, jitter, jitter buffer loss, and lost data.

Resource Objects

Call Perf object

Call Perf proxy object

When you run this script on an agent computer that acts as proxy for multiple remote computers, AppManager creates only one job that drives the tests for all talkers on that computer. These tests run simultaneously. Running multiple tests at one time can take an undesirable toll on your bandwidth resources. Use the Objects tab on the Knowledge Script Properties dialog box to include or exclude remote resources from the tests.

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Select listener(s)	Select the listener computers from the Select Desired Computers dialog box.
Collect data?	Select **Yes** to collect data about MOS, R-value, delay, jitter, jitter buffer loss, and lost data for charts and graphs. The default is Yes.
Collect network delay data?	Select **Yes** to collect data about network delay for charts and graphs. The default is unselected.
Configuration Settings	
Test duration	Specify the duration of a test event in seconds, between one and 300. The default is 60 seconds.

Parameter	How To Set It
Service Quality	Select a DiffServ (Differentiated Services) codepoint for classifying the bits in the IP header: • **None**. Default setting. No special treatment is given to packets. • **EF0-101000**. Deprecated Expedited Flow codepoint in use by most phones. Equivalent to the TOS "CRITIC/ECP" setting reserved for voice. • **EF-101110**. Expedited Forwarding per-hop behavior (PHB) codepoint, represents the highest-priority service. • **AF-011000**. Deprecated Assured Flow per-hop behavior (PHB) codepoint, represents a medium-quality service. Equivalent to the TOS "flash" setting. • **AF11-001010** (Assured Forwarding, Class 1, low drop precedence) • **AF12 - 001100** (Assured Forwarding, Class 1, medium drop precedence) • **AF13-001110** (Assured Forwarding, Class 1, high drop precedence) • **AF2 -010010** (Assured Forwarding, Class 2, low drop precedence) • **AF22-010100** (Assured Forwarding, Class 2, medium drop precedence) • **AF23-010110** (Assured Forwarding, Class 2, high drop precedence) • **AF31 011010** (Assured Forwarding, Class 3, low drop precedence) • **AF32-011100** (Assured Forwarding, Class 3, medium drop precedence) • **AF33-011110** (Assured Forwarding, Class 3, high drop precedence) • **AF4 -100010** (Assured Forwarding, Class 4, low drop precedence) • **AF42-100100** (Assured Forwarding, Class 4, medium drop precedence) • **AF43-100110** (Assured Forwarding, Class 4, high drop precedence) • **802.1p-011** (For medium-priority traffic, often used for call setup packets) • **802.1p-101** (For high-priority traffic, recommended for VoIP data packets)
Voice activity rate	Specify a voice activity rate percentage. For example, enter 50 to indicate that data is being sent during 50% of a call's duration. The default is 50%.
Delay between voice datagrams	Specify a delay between voice datagrams. The delay determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Use silence suppression?	Select **Yes** to enable silence suppression, which means that no data is sent during periods of “call silence” (i.e. when no one is talking). The default is unselected.
Advanced Configuration Settings	
Absolute jitter buffer size	Specify the size of the absolute jitter buffer in milliseconds. The jitter buffer size is a critical component of the MOS calculation. For example, a jitter buffer of 43 ms could hold two 20-ms datagram packets and allow for three extra milliseconds of variability. The default is 40 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Event Notification	

Parameter	How To Set It
Raise event if test fails?	Select **Yes** to raise an event if the VoIP test does not complete successfully. The default is Yes.
Event severity when test fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the VoIP test does not complete successfully. The default is 5.
Raise event if MOS/R-value falls below threshold	Select **Yes** to raise an event if the MOS score or R-value falls below the threshold that you set. The default is Yes.
VoIP quality metric for event	Select the VoIP quality metric you want to use for the VoIP test. The default is MOS. • **MOS**. The Mean Opinion Score (MOS) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. The MOS is calculated based on measured items plus jitter buffer size. The jitter buffer size is constant based on the codec/script. Only one jitter buffer size is specified and used throughout the test. • **R-value**. A single score that is derived from delays and equipment impairment factors. An R-value can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor).
Threshold - Minimum MOS	Specify the minimum Mean Opinion Score (MOS) that must be reached to prevent an event from being raised The default is 3.60.
Threshold - Minimum R-value	Specify the minimum acceptable R-value that must be reached to prevent an event from being raised. The default is 70.
Event severity when VoIP quality falls below threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which MOS or R-value falls below the threshold that you set. The default is 5.
Raise event if delay exceeds threshold?	Select **Yes** to raise an event if delay exceeds the threshold that you set. The default is Yes.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets. The default is 400 ms.
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold that you set. The default is 15.
Raise event if jitter exceeds threshold?	Select **Yes** to raise an event if jitter exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets. The default is 60 ms.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold that you set. The default is 15.
Raise event if jitter buffer loss exceeds threshold?	Select **Yes** to raise an event if jitter buffer loss exceeds the threshold that you set. The default is Yes.
Threshold - Maximum jitter buffer loss	Specify the maximum percentage of jitter buffer loss that can occur before an event is raised. The default is 1.0%. Jitter buffer loss is the amount of data that is lost when jitter exceeds that which the jitter buffer can hold. Jitter buffer loss affects call clarity, which affects the overall MOS score.
Event severity when jitter buffer loss exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter buffer loss exceeds the threshold that you set. The default is 15.
Raise event if lost data exceeds threshold?	Select **Yes** to raise an event if lost data exceeds the threshold that you set. The default is Yes.

Parameter	How To Set It
Threshold - Maximum lost data	Specify the maximum percentage of lost data that can occur before an event is raised. The default is 1.0%. To calculate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold that you set. The default is 15.

CiscoSAA_G711a

Use this Knowledge Script to run a VoIP test between Cisco SAA-enabled routers using the G.711a codec, which uses the A-law for companding, a popular standard in Europe. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for delay, jitter, and lost data.

Resource Object

Cisco SAA object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Select **y** to collect data about delay, jitter, and lost data for charts and graphs. The default is y.
Select target router(s)	Select the target routers (listeners) that you want to include in the VoIP test.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The default is 400 ms. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. The default is 60 ms. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets.
Threshold - Maximum lost data	Specify the maximum percentage of data that can be lost before an event is raised. The default is 1.0%. To generate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when test fails	Set a severity level, between 1 and 40, to indicate the importance of an event in which the VoIP test fails. The default is 5. Select 0 if you do not want to raise an event.
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Test duration	Specify the duration of a test event in seconds. The default is 60 seconds.

Parameter	How To Set It
Service Quality	Select a quality of service (QoS) option for the IP Type of Service (TOS) precedence bits in the IP header: • **None - 000**. This is the default setting. No special treatment is given to packets. • **DiffServAF - 011**. The DiffServ Assured Flow setting represents a medium-quality service. This setting is equivalent to the TOS "flash" setting. • **DiffServEF - 101**. The DiffServ Expedited Flow setting represents the highest-priority service. This setting is equivalent to the TOS "CRITIC/ECP" setting reserved for voice.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Delay between voice datagrams	Specify a delay in milliseconds between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.

CiscoSAA_G711u

Use this Knowledge Script to run a VoIP test between Cisco SAA-enabled routers using the G.711u codec, which uses the u-law for companding, the most frequently used method in the USA. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for delay, jitter, and lost data.

Resource Object

Cisco SAA object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Select **y** to collect data about delay, jitter, and lost data for charts and graphs. The default is y.
Select target router(s)	Select the target routers (listeners) that you want to include in the VoIP test.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The default is 400 ms. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. The default is 60 ms. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets.
Threshold - Maximum lost data	Specify the maximum percentage of data that can be lost before an event is raised. The default is 1.0%. To generate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when test fails	Set a severity level, between 1 and 40, to indicate the importance of an event in which the VoIP test fails. The default is 5. Select 0 if you do not want to raise an event.
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.

Parameter	How To Set It
Test duration	Specify the duration of a test event in seconds. The default is 60 seconds.
Service Quality	Select a quality of service (QoS) option for the IP Type of Service (TOS) precedence bits in the IP header: • **None - 000**. This is the default setting. No special treatment is given to packets. • **DiffServAF - 011**. The DiffServ Assured Flow setting represents a medium-quality service. This setting is equivalent to the TOS "flash" setting. • **DiffServEF - 101**. The DiffServ Expedited Flow setting represents the highest-priority service. This setting is equivalent to the TOS "CRITIC/ECP" setting reserved for voice.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Delay between voice datagrams	Specify a delay in milliseconds between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.

CiscoSAA_G723.1-ACELP

Use this Knowledge Script to run a VoIP test between Cisco SAA-enabled routers using the G.723.1-ACELP codec, which uses the conjugate structure algebraic code excited linear predictive compression (ACELP) algorithm. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for delay, jitter, and lost data.

Resource Object

Cisco SAA object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Select **y** to collect data about delay, jitter, and lost data for charts and graphs. The default is y.
Select target router(s)	Select the target routers (listeners) that you want to include in the VoIP test.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The default is 400 ms. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. The default is 60 ms. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets.
Threshold - Maximum lost data	Specify the maximum percentage of data that can be lost before an event is raised. The default is 1.0%. To generate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when test fails	Set a severity level, between 1 and 40, to indicate the importance of an event in which the VoIP test fails. The default is 5. Select 0 if you do not want to raise an event.
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.

Parameter	How To Set It
Test duration	Specify the duration of a test event in seconds. The default is 60 seconds.
Service Quality	Select a quality of service (QoS) option for the IP Type of Service (TOS) precedence bits in the IP header: • **None - 000**. This is the default setting. No special treatment is given to packets. • **DiffServAF - 011**. The DiffServ Assured Flow setting represents a medium-quality service. This setting is equivalent to the TOS "flash" setting. • **DiffServEF - 101**. The DiffServ Expedited Flow setting represents the highest-priority service. This setting is equivalent to the TOS "CRITIC/ECP" setting reserved for voice.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Delay between voice datagrams	Specify a delay in milliseconds between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.

CiscoSAA_G723.1-MPMLQ

Use this Knowledge Script to run a VoIP test between Cisco SAA-enabled routers using the G.723.1-MPMLQ codec, which uses the multipulse maximum likelihood quantization (MPMLQ) compression algorithm. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for delay, jitter, and lost data.

Resource Object

Cisco SAA object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Select **y** to collect data about delay, jitter, and lost data for charts and graphs. The default is y.
Select target router(s)	Select the target routers (listeners) that you want to include in the VoIP test.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The default is 400 ms. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. The default is 60 ms. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets.
Threshold - Maximum lost data	Specify the maximum percentage of data that can be lost before an event is raised. The default is 1.0%. To generate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when test fails	Set a severity level, between 1 and 40, to indicate the importance of an event in which the VoIP test fails. The default is 5. Select 0 if you do not want to raise an event.
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.

Parameter	How To Set It
Test duration	Specify the duration of a test event in seconds. The default is 60 seconds.
Service Quality	Select a quality of service (QoS) option for the IP Type of Service (TOS) precedence bits in the IP header: • **None - 000**. This is the default setting. No special treatment is given to packets. • **DiffServAF - 011**. The DiffServ Assured Flow setting represents a medium-quality service. This setting is equivalent to the TOS "flash" setting. • **DiffServEF - 101**. The DiffServ Expedited Flow setting represents the highest-priority service. This setting is equivalent to the TOS "CRITIC/ECP" setting reserved for voice.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Delay between voice datagrams	Specify a delay in milliseconds between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.

CiscoSAA_G726

Use this Knowledge Script to run a VoIP test between Cisco SAA-enabled routers using the G.726 codec, a waveform coder that uses Adaptive Differential Pulse Code Modulation (ADPCM). ADPCM is a variation of pulse code modulation (PCM), which sends only the difference between two adjacent samples, producing a lower bit rate. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for delay, jitter, and lost data.

Resource Object

Cisco SAA object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Select **y** to collect data about delay, jitter, and lost data for charts and graphs. The default is y.
Select target router(s)	Select the target routers (listeners) that you want to include in the VoIP test.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The default is 400 ms. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. The default is 60 ms. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets.
Threshold - Maximum lost data	Specify the maximum percentage of data that can be lost before an event is raised. The default is 1.0%. To generate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when test fails	Set a severity level, between 1 and 40, to indicate the importance of an event in which the VoIP test fails. The default is 5. Select 0 if you do not want to raise an event.
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.

Parameter	How To Set It
Test duration	Specify the duration of a test event in seconds. The default is 60 seconds.
Service Quality	Select a quality of service (QoS) option for the IP Type of Service (TOS) precedence bits in the IP header: • **None - 000**. This is the default setting. No special treatment is given to packets. • **DiffServAF - 011**. The DiffServ Assured Flow setting represents a medium-quality service. This setting is equivalent to the TOS "flash" setting. • **DiffServEF - 101**. The DiffServ Expedited Flow setting represents the highest-priority service. This setting is equivalent to the TOS "CRITIC/ECP" setting reserved for voice.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Delay between voice datagrams	Specify a delay in milliseconds between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.

CiscoSAA_G729

Use this Knowledge Script to run a VoIP test between Cisco SAA-enabled routers using the G.729 codec, which offers compression with high quality. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for delay, jitter, and lost data.

Resource Object

Cisco SAA object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Select **y** to collect data about delay, jitter, and lost data for charts and graphs. The default is y.
Select target router(s)	Select the target routers (listeners) that you want to include in the VoIP test.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The default is 400 ms. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. The default is 60 ms. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets.
Threshold - Maximum lost data	Specify the maximum percentage of data that can be lost before an event is raised. The default is 1.0%. To generate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when test fails	Set a severity level, between 1 and 40, to indicate the importance of an event in which the VoIP test fails. The default is 5. Select 0 if you do not want to raise an event.
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Test duration	Specify the duration of a test event in seconds. The default is 60 seconds.

Parameter	How To Set It
Service Quality	Select a quality of service (QoS) option for the IP Type of Service (TOS) precedence bits in the IP header: • **None - 000**. This is the default setting. No special treatment is given to packets. • **DiffServAF - 011**. The DiffServ Assured Flow setting represents a medium-quality service. This setting is equivalent to the TOS "flash" setting. • **DiffServEF - 101**. The DiffServ Expedited Flow setting represents the highest-priority service. This setting is equivalent to the TOS "CRITIC/ECP" setting reserved for voice.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Delay between voice datagrams	Specify a delay in milliseconds between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.

CiscoSAA_G729A

Use this Knowledge Script to run a VoIP test between Cisco SAA-enabled routers using the G.729 Annex A codec, which offers compression with high quality. This script raises an event if a threshold is exceeded. In addition, this script generates data streams for delay, jitter, and lost data.

Resource Object

Cisco SAA object

Default Schedule

By default, this script runs every 15 minutes.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Collect data?	Select **y** to collect data about delay, jitter, and lost data for charts and graphs. The default is y.
Select target router(s)	Select the target routers (listeners) that you want to include in the VoIP test.
Threshold - Maximum delay	Specify the maximum amount of delay that can occur before an event is raised. The default is 400 ms. The delay is calculated on each packet. The delay of the test is the average of the delay for all packets.
Threshold - Maximum jitter	Specify the maximum amount of jitter that can occur before an event is raised. The default is 60 ms. Jitter indicates the variation in packet arrival time. The jitter for the test is the average of the jitter between all packets.
Threshold - Maximum lost data	Specify the maximum percentage of data that can be lost before an event is raised. The default is 1.0%. To generate this percentage, the script divides the number of datagrams lost by the number of datagrams sent.
Event severity when test fails	Set a severity level, between 1 and 40, to indicate the importance of an event in which the VoIP test fails. The default is 5. Select 0 if you do not want to raise an event.
Event severity when delay exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which delay exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when jitter exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which jitter exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Event severity when lost data exceeds threshold	Set a severity level, between 1 and 40, to indicate the importance of an event in which lost data exceeds the threshold. The default is 15. Select 0 if you do not want to raise an event.
Test duration	Specify the duration of a test event in seconds. The default is 60 seconds.

Parameter	How To Set It
Service Quality	Select a quality of service (QoS) option for the IP Type of Service (TOS) precedence bits in the IP header: • **None - 000**. This is the default setting. No special treatment is given to packets. • **DiffServAF - 011**. The DiffServ Assured Flow setting represents a medium-quality service. This setting is equivalent to the TOS "flash" setting. • **DiffServEF - 101**. The DiffServ Expedited Flow setting represents the highest-priority service. This setting is equivalent to the TOS "CRITIC/ECP" setting reserved for voice.
Source port number	Specify the port number of the test source computer. Accept the default of AUTO to automatically locate the port number.
Destination port number	Specify the port number of the test destination computer. Accept the default of AUTO to automatically locate the port number.
Delay between voice datagrams	Specify a delay in milliseconds between voice datagrams. The delay between datagrams determines the size of the datagram packets. A delay of 20 ms means that accumulated data is sent every 20 milliseconds. A smaller delay value results in smaller, more frequent datagrams that increase processing overhead; a larger delay value results in fewer, larger datagrams that increase delay. The default is 20 ms.
Additional fixed delay	Specify any additional fixed delay in milliseconds. Use this parameter to add a delay value from a known, constant source. For instance, if your test equipment adds 10 ms of delay to each datagram, enter 10 here. The default is 0 ms.

Report_Configuration

Use this Knowledge Script to summarize the VoIP Quality configuration for selected computers.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data Source	
Computer selection by	Select the computers that you want to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select computers	Select the view in which you want to see the results. The default is Master.
Report Settings	
Include parameter help card?	Select **y** to include a table in the report that lists parameter settings for the script. The default is y.
Select output folder	Select the name and location of the folder in which the report will be saved. The default is VoIPQuality_Configuration.
Add job ID to output folder name?	Select **y** to add the job ID to the name of the output folder. The default is n. The job ID is helpful to make the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Select and enter miscellaneous report properties in the Report Properties dialog box.
Add time stamp to title	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	This script automatically raises an event if the report is not generated successfully. Select **y** to raise an event when the report is generated successfully. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_GroupSummary

Use this Knowledge Script to summarize average VoIP Quality data stream values (MOS, R-value, availability, delay, jitter, jitter buffer loss, lost data) for a specified period.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data Source	
Values grouped by	Select the category by which you want to group data for display in the report. The default is Talker.
Select Knowledge Script(s)	Select the Knowledge Scripts that generated the data that you want to include in the report.
Computer selection by	Select the category by which you want to select the computers that you want to include in the report: View, Server Group, or Computer. The default is View.
Select computers	Select the computers that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Chart Thresholds	
MOS threshold	Specify the MOS threshold to display on the MOS charts in the report. The default is 0.000.
R-value threshold	Specify the R-value threshold to display on the R-value charts in the report. The default is 0.000.
Availability threshold	Specify the Availability threshold to display on the Availability charts in the report. The default is 0%.
Delay threshold	Specify the Delay threshold to display on the Delay charts in the report. The default is 0 ms.
Jitter threshold	Specify the Jitter threshold to display on the Jitter charts in the report. The default is 0 ms.
Percent Jitter Buffer Loss threshold	Specify the Jitter Buffer Loss threshold to display on the Jitter Buffer Loss charts in the report. The default is 0.000%.
Percent Lost Data threshold	Specify the Lost Data threshold to display on the Percent Lost Data charts in the report. The default is 0.000%.
Report Settings	
Include parameter card?	Select **y** to include a table in the report that lists parameter settings for the report script. The default is y.

Parameter	How To Set It
Include charts?	Select **y** to include a chart in the report. The default is y.
Include table?	Select **y** to include a table of information in the report. The default is y.
Select chart style	Select and enter chart properties in the Chart Settings dialog box. The default style is Bar.
Select output folder	Select the name and location of the folder in which the report will be saved. The default name is VoIPQualityGroupSum.
Add job ID to output folder name?	Select **y** to add the job ID to the name of the output folder. The default is n. The job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Select and enter report properties in the Report Properties dialog box. The default name is VoIP Quality Group Summary.
Add time stamp to title	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	This script automatically raises an event if the report is not generated successfully. Select **y** to raise an event when the report is generated successfully. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_MOSAvailMatrix

Use this Knowledge Script to summarize average MOS and availability between a talker and a listener within a selected period.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data Source	
Select Knowledge Script(s)	Select the Knowledge Scripts that generated the data that you want to include in the report.
Computer selection by	Select the category by which you want to select the computers that you want to include in the report: View, Server Group, or Computer. The default is View.
Select computers	Select the computers that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	
Decimal accuracy for % values	Specify the number of decimal places that you want to see in the percentage values generated by this report. The default is 3.
Include parameter card?	Select **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default name is VoIPQuality_MOSAvailMatrix
Add job ID to output folder name?	Select **y** to add the job ID to the name of the output folder. The default is n. The job is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Select and enter report properties in the Report Properties dialog box. The default report name is VoIP Quality MOS - Availability Matrix.
Add time stamp to title	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	This script automatically raises an event if the report is not generated successfully. Select **y** to raise an event when the report is generated successfully. The default is y.

Parameter	How To Set It
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_MOSSummary

Use this Knowledge Script to summarize average MOS quality within a group within a selected time range.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data Source	
Calls grouped by	Select the category by which you want to group data for display in the report. The default is Talker.
Select Knowledge Script(s)	Select the Knowledge Scripts that generated the data that you want to include in the report.
Computer selection by	Select the category by which you want to select the computers that you want to include in the report: View, Server Group, or Computer. The default is View.
Select computers	Select the computers that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Chart Thresholds	
Good-Acceptable threshold	Specify a MOS value below which the call is acceptable and equal to or above which the call is good. This value appears on the chart as a thick horizontal line. The default is 4.030.
Acceptable-Poor threshold	Specify a MOS value below which the call is poor and above which the call is acceptable. This value appears on the chart as a thick horizontal line. The default is 3.600.
Chart Settings	
Chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Horizontal chart?	Select **y** to create a horizontal bar chart or accept the default to create a vertical bar chart.
Chart color scheme	Select a color scheme template. The default is NetIQ.
Report Settings	
Include parameter card?	Select **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Select **y** to include a chart in the report. The default is y.
Include table?	Select **y** to include a table of information in the report. The default is y.

Parameter	How To Set It
Select output folder	Select the name and location of the folder in which the report will be output. The default name is VoIPQualityMOSSum.
Add job ID to output folder name?	Select **y** to add the job ID to the name of the output folder. The default is n. The job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Select and enter report properties in the Report Properties dialog box. The default name is VoIP Quality MOS Summary.
Add time stamp to title	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	This script automatically raises an event if the report is not generated successfully. Select **y** to raise an event when the report is generated successfully. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successful. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_RvalueSummary

Use this Knowledge Script to summarize average R-value quality within a group within a selected time range.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data Source	
Calls grouped by	Select the category by which you want to group data for display in the report. The default is Talker.
Select Knowledge Script(s)	Select the Knowledge Scripts that generated the data that you want to include in the report.
Computer selection by	Select the category by which you want to select the computers that you want to include in the report: View, Server Group, or Computer. The default is View.
Select computers	Select the computers that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Chart Thresholds	
Good-Acceptable threshold	Specify an R-value below which the call is acceptable and equal to or above which the call is good. This value appears on the chart as a thick horizontal line. The default is 80.0.
Acceptable-Poor threshold	Specify an R-value below which the call is poor and above which the call is acceptable. This value appears on the chart as a thick horizontal line. The default is 70.0.
Chart Settings	
Chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Horizontal chart?	Select **y** to create a horizontal bar chart or accept the default to create a vertical bar chart.
Chart color scheme	Select a color scheme template. The default is NetIQ.
Report Settings	
Include parameter card?	Select **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Select **y** to include a chart in the report. The default is y.
Include table?	Select **y** to include a table of information in the report. The default is y.

Parameter	How To Set It
Select output folder	Select the name and location of the folder in which the report will be output. The default name is VoIPQualityRvalueSum.
Add job ID to output folder name?	Select **y** to add the job ID to the name of the output folder. The default is n. The job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Select and enter report properties in the Report Properties dialog box. The default name is VoIP Quality R-value Summary.
Add time stamp to title	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	This script automatically raises an event if the report is not generated successfully. Select **y** to raise an event when the report is generated successfully. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_TimeDetail

Use this Knowledge Script to summarize the average values by minute of the VoIP Quality data streams (MOS, R-value, availability, delay, jitter, jitter buffer loss, lost data) within a selected period.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data Source	
Select Knowledge Scripts	Select the Knowledge Scripts that generated the data that you want to include in the report.
Computer selection by	Select the category by which you want to select the computers that you want to include in the report: View, Server Group, or Computer. The default is View.
Select computers	Select the computers that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Aggregate by n minutes	Specify the interval in minutes in which time data will be grouped. The default is 30 minutes.
Chart Thresholds	
MOS threshold	Specify the MOS threshold to display on the MOS charts in the report. The default is 0.000.
R-value threshold	Specify the R-value threshold to display on the R-value charts in the report. The default is 0.000.
Availability threshold	Specify the Availability threshold to display on the Availability charts in the report. The default is 0%.
Delay threshold	Specify the Delay threshold to display on the Delay charts in the report. The default is 0 ms.
Jitter threshold	Specify the Jitter threshold to display on the Jitter charts in the report. The default is 0 ms.
Percent Jitter Buffer Loss threshold	Specify the Jitter Buffer Loss threshold to display on the Jitter Buffer Loss charts in the report. The default is 0.000%.
Percent Lost Data threshold	Specify the Lost Data threshold to display on the Percent Lost Data charts in the report. The default is 0.000%.
Report Settings	
Include parameter card?	Select **y** to include a table in the report that lists parameter settings for the report script. The default is y.

Parameter	How To Set It
Include charts?	Select **y** to include a chart in the report. The default is y.
Include table?	Select **y** to include a table of information in the report. The default is y.
Select chart style	Select and enter chart properties in the Chart Settings dialog box. The default style is Line.
Select output folder	Select the name and location of the folder in which the report will be output. The default name is VoIPQualityTimeDetail.
Add job ID to output folder name?	Select **y** to add the job ID to the name of the output folder. The default is n. The job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Select and enter report properties in the Report Properties dialog box. The default name is VoIP Quality Time Detail.
Add time stamp to title	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	This script automatically raises an event if the report is not generated successfully. Select **y** to raise an event when the report is generated successfully. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Report_VoIPQualitySummary

Use this Knowledge Script to summarize VoIP quality statistics (MOS, R-value, delay, jitter, jitter buffer loss, and lost data) within a group within a selected period.

Resource Object

Report agent

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
Data Source	
Calls grouped by	Select the category by which you want to group data for display in the report. The default is Talker.
Select Knowledge Script(s)	Select the Knowledge Scripts that generated the data that you want to include in the report.
Computer selection by	Select the category by which you want to select the computers that you want to include in the report: View, Server Group, or Computer. The default is View.
Select computers	Select the computers that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Chart Thresholds	
Good-Acceptable MOS threshold	Specify the MOS threshold for the good-to-acceptable range to display in the report. The default is 4.030.
Acceptable-Poor MOS threshold	Specify the MOS threshold for the acceptable-to-poor range to display in the report. The default is 3.600.
Good-Acceptable R-value threshold	Specify the R-value threshold for the good-to-acceptable range to display in the report. The default is 80.0.
Acceptable-Poor R-value threshold	Specify the R-value threshold for the acceptable-to-poor range to display in the report. The default is 70.0.
Good-Acceptable delay threshold	Specify the delay threshold for the good-to-acceptable range to display in the report. The default is 150 ms.
Acceptable-Poor delay threshold	Specify the delay threshold for the acceptable-to-poor range to display in the report. The default is 400 ms.
Good-Acceptable jitter threshold	Specify the jitter threshold for the good-to-acceptable range to display in the report. The default is 40 ms.
Acceptable-Poor jitter threshold	Specify the jitter threshold for the acceptable-poor range to display in the report. The default is 60 ms.

Parameter	How To Set It
Good-Acceptable packet loss threshold	Specify the packet loss threshold for the good-acceptable range to display in the report. The default is 0.5%.
Acceptable-Poor packet loss threshold	Specify the packet loss threshold for the acceptable-poor range to display in the report. The default is 1.0%.
Good-Acceptable jitter buffer loss threshold	Specify the jitter buffer loss threshold for the good-acceptable range to display in the report. The default is 0.5%.
Acceptable-Poor jitter buffer loss threshold	Specify the jitter buffer loss threshold for the acceptable-poor range to display in the report. The default is 1.0%.
Chart Settings	
Chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Horizontal chart?	Select **y** to create a horizontal bar chart or accept the default to create a vertical bar chart.
Chart color scheme	Select a color scheme template. The default is NetIQ.
Report Settings	
Include parameter card?	Select **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include charts?	Select **y** to include a chart in the report. The default is y.
Include table?	Select **y** to include a table of information in the report. The default is y.
Select output folder	Select the name and location of the folder in which the report will be output. The default name is VoIPQualityCallSum.
Add job ID to output folder name?	Select **y** to add the job ID to the name of the output folder. The default is n. The job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Select and enter report properties in the Report Properties dialog box. The default name is VoIP Quality Summary.
Add time stamp to title	Select **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp consists of the date and time the report was generated. Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event if report succeeds?	This script automatically raises an event if the report is not generated successfully. Select **y** to raise an event when the report is generated successfully. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated successfully. The default is 35.
Event severity when report has no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

Reviewing Call Performance Metrics

The VoIPQuality_CallPerf and VoIPQuality_CiscoSAA Knowledge Scripts generate data streams, based on some or all of the following call performance metrics, for use in graphs and reports.

Metric	Description
MOS	The Mean Opinion Score (MOS) is an overall score representing the quality of a call. The MOS is a number between 1 and 5. A MOS of 5 is excellent; a MOS of 1 is unacceptably bad. The MOS is calculated based on measured items plus jitter buffer size. The jitter buffer size is constant based on the codec. Jitter buffers minimize the call disruptions from delay and jitter. However, jitter buffers themselves contribute to the overall delay experienced by the call. Additionally, in situations with high network delay, jitter buffers can cause data to be lost. Thus the jitter buffer must be factored into the MOS calculation. NetIQ uses a modified version of the ITU (International Telecommunications Union) G.107 standard E-model equation to calculate the MOS. The E-model, developed by the European Telecommunications Standards Institute (ETSI), has become ITU standard G.107. This algorithm is used to evaluate the quality of a transmission by factoring in the "mouth to ear" characteristics of a speech path. **Note** AppManager for Cisco SAA does not generate MOS metrics.
R-value	Defined by ITU (International Telecommunication Union) recommendation G.107, the E-model is a complex calculation, the output of which is a single score called an R-value that is derived from delays and equipment impairment factors. An R-value can be mapped to an estimated MOS. R-values range from 100 (excellent) to 0 (poor). An estimated MOS can be directly calculated from an R-value. **Note** AppManager for Cisco SAA does not generate R-value metrics.
Delay	Measured in milliseconds, delay is perhaps the most common hindrance to VoIP call quality. The delay is calculated on each packet. This value includes all delay factors between the endpoints. The end-to-end delay, or latency, as measured between the endpoints is a key factor in determining voice over IP call quality. The AppManager delay measurement is taken for datagrams traveling between the endpoints in a single direction and includes the following factors: • **Network delay in one direction**—Datagram's RTP timestamp subtracted from time it was received by Endpoint 2. Endpoints must synchronize their high-precision timers to calculate one-way delay. This delay factor actually includes the propagation delay (time spent on the actual network) and the transport delay (time spent getting through intermediate network devices). • **Packetization delay**—Fixed value; dependant on selected codec. • **Jitter buffer delay**—Fixed value; dependant on type and size of configured jitter buffer. • **Additional fixed delay**—Fixed value; user-configured. Most callers notice delay when it exceeds 250ms. ITU-T standard G.114 specifies 150ms as the maximum one-way delay that is tolerable for high-quality VoIP.

Metric	Description
Jitter	As simulated calls run during a VoIP quality test, the endpoints calculate jitter, a factor known to adversely affect call quality. Jitter is also called delay variation, and it indicates the variance of the arrival rate of datagrams sent during a simulated VoIP call. When a datagram is sent, the sender (one of the endpoints) gives it a timestamp. When a datagram is received, the receiver adds another timestamp. These two timestamps are used to calculate the datagram's transit time. If the transit times for datagrams within the same call are different, the call contains jitter. In a video application, jitter manifests itself as a flickering image, while in a telephone call, its effect may be similar to the effect of packet loss: some words may be missing or garbled. The amount of jitter in a call depends on the degree of difference between the datagrams' transit times. If the transit time for all datagrams is the same (no matter how long it took for the datagrams to arrive), the call contains no jitter. If the transit times differ slightly, the call contains some jitter. Jitter values in excess of 50ms probably indicate poor call quality. They provide a short-term measurement of network congestion and can also show the effects of queuing within the network.
Jitter Buffer Loss	Jitter buffer loss is the amount of data that is lost when jitter exceeds that which the jitter buffer can hold. Jitter buffer loss affects call clarity, which affects the overall MOS score. Jitter buffers smooth out variations in calls by holding some datagrams to feed them to the application sequentially. Datagrams that are not contained by the jitter buffer due to excessive delay variation would be lost to the application and are thus called jitter buffer lost datagrams. This statistic includes datagrams with delay too great for the jitter buffer you set ("overruns") as well as those that arrive too quickly while the jitter buffer is still full and must be discarded ("underruns"). Any jitter detected in the call is compared to the size of the jitter buffer in the call script. Jitter buffer lost datagrams are then expressed as a percentage of all datagrams sent. AppManager uses the jitter buffer loss statistic when calculating a MOS for simulated VoIP traffic sent between the target devices.
Percent Lost Data	When a datagram is lost during a VoIP transmission, you can lose an entire syllable or word in a conversation. Obviously, data loss can severely impair call quality. AppManager therefore includes data loss as a call quality impairment factor in calculating the MOS of each simulated VoIP call. To measure data loss, the sending endpoint reports to the receiving endpoint how many bytes it sent, and the receiver compares that value to the amount received to determine lost data. Because *packet loss concealment* (PLC) is enabled by default in the G.711 codecs, call quality is less adversely affected if any data is lost during the VoIP test. PLC makes the codec itself more expensive to manufacture, but does not otherwise add delay or have other bad side effects.

Diagnosing VoIP Quality Problems

AppManager includes Knowledge Scripts that monitor and detect problems with VoIP quality and call quality. These scripts raise informational events as a result of the detected problems. By using NetIQ Vivinet Diagnostics and AppManager together, you have the means to diagnose more precisely any problems with VoIP quality between phones, endpoints, or other target devices such as routers and gateways.

Using an existing methodology (launching an Action script based on an event), the VoIPQuality_CallPerf Knowledge Scripts can run the Action_DiagnoseVoIPQuality Knowledge Script, which in turn launches Vivinet Diagnostics to diagnose the problem when MOS, R-value, delay, jitter, jitter buffer loss, and percentage of lost data exceed their thresholds.

The Action script runs by default only if Vivinet Diagnostics version 1.1 or later is installed on the computer on which it runs.

To enable a VoIPQuality_CallPerf Knowledge Script to launch Vivinet Diagnostics:

1. In the script's Properties dialog box, click the **Actions** tab. Action_DiagnoseVoIPQuality is selected by default.
2. Click **Properties**.
3. Enter values for all parameters. For more information about the parameter values, click **Help** on the Properties for Action_DiagnoseVoIPQuality dialog box.
4. Continue entering values on the other tabs of the Properties dialog box, or click **OK** to run the job.

Reviewing Quality of Service

In order for VoIP users to receive an acceptable level of voice quality, VoIP traffic must be given priority over other kinds of network traffic, such as data. The main goal of *Quality of Service* (QoS) is to ensure that VoIP traffic receives the preferential treatment it deserves, thereby reducing or eliminating the delay of voice packets that travel across a network.

In order to work with multiple types of network traffic, QoS first *classifies* the traffic, and then *handles* it. Once traffic is sorted into classes, QoS can determine how the traffic should be treated.

One QoS standard for sorting traffic is *DiffServ* (Differentiated Services). DiffServ sorts packets into groups that have similar QoS requirements and then gives those groups the required treatment at every hop in the network, also known as the *per-hop behavior* (PHB). DiffServ uses the second byte (eight bits) in the IP header to define and sort a packet. Of the eight bits, the last two are reserved for future use. DiffServ uses only the first six bits (the *Differentiated Services* [DS] field) in classifying a packet into one of three *codepoints*: Best Effort, Expedited Forwarding, and Assured Forwarding.

DiffServ-enabled routers can subdivide networks into DiffServ (DS) domains, within which all IP traffic competes for a finite share of bandwidth determined by a committed information rate, or CIR. To ensure that traffic that exceeds the CIR is still delivered without compromising the performance of high-priority traffic, packets within a DS domain are placed into PHB groups, including Expedited Forwarding and Assured Forwarding. Of these two groups, Expedited Forwarding receives slightly lower drop precedence and slightly higher bandwidth allocation than Assured Forwarding.

These groups allow for very exact policy-based QoS: they can be further subdivided to determine which packets are least likely to be dropped and most likely to be forwarded quickly despite congestion. Assured Forwarding includes four classes, AF1-AF4. Within each class, three subclasses may be defined, with increasing drop precedence. For example, AF1 may be the highest class of traffic, but within that class, AF13 will be dropped before AF11 or AF12.

Two DiffServ settings once used as part of the standard implementation may soon be deprecated, or rendered obsolete. Those settings, Expedited Flow and Assured Flow, used only the first three bits of the DiffServ codepoint, the type of service (TOS) bits. More recent DiffServ implementations use all six bits, for a total of 64 possible settings.

Note

TOS (Type of Service) is the previous name used to identify the second byte of the IP header. Used in early TCP/IP specs, TOS is described in RFC 791. In more recent TCP/IP specs, the same byte is referred to as the DS field, which is described in RFC2474.

IEEE 802.1p is an OSI Layer 2 standard for prioritizing and queuing network traffic at the data link/MAC sub-layer. It can also be defined as best-effort QoS at Layer 2. 802.1p traffic is classified and sent to the destination with no bandwidth reservation.

The three-bit Prioritization field in the 802.1p tag establishes eight levels of priority, similar to the IP Precedence bits. A level-eight priority is the highest, and is thus reserved for router-update traffic. However, AppManager supports only the two priority levels that are appropriate for VoIP traffic:

- 011~(3) For medium-priority traffic. Often used for call setup packets.
- 101~(5) For high-priority traffic. Recommended for VoIP data packets.

Network adapters and switches route traffic based on the priority level. The hardware itself-usually a NIC card or an IP phone-does the tagging. Many recently developed IP phones are marking voice packets with a priority of five (101).

Note

Some older switches support just two or three priority queues, so their implementation of 802.1p does not support all of the eight priority levels in the IEEE 802.1p specification. Such switches place 802.1p values of 0 through 3 in a low-priority queue, and priority levels 4 through 7 in a high-priority queue, using only two different priority levels.

When monitoring call performance with AppManager, you can run a VoIP test using a DiffServ codepoint and one of the VoIP Quality Knowledge Scripts.

Chapter 71
WebLogicSvrUnix Knowledge Scripts

The WebLogicSvrUNIX category provides the following Knowledge Scripts for monitoring WebLogic Server running on UNIX.

From the Knowledge Script view of Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
Availability	Monitors the availability of a WebLogic Server.
HealthCheck	Verifies that a WebLogic Server is running, can respond to requests, and can accept connections from clients.
LogAccessLog	Returns the number of entries in the WebLogic Server's `access.log` since the last sample that match the search criteria. Provides a way to monitor HTTP requests and sessions.
LogAccessLogSetPath	Sets the absolute pathname for a Web server log file.
LogWebLogic	Monitors entries that are added to the log for a WebLogic Server.
LogWebLogicSetPath	Sets the absolute pathname for a WebLogic Server log file.
Memory	Monitors the physical and virtual memory use of a WebLogic Server.
SecurityUserLockout	Monitors statistics on the number of users locked out because invalid usernames and/or passwords were supplied at login.
ServerCPU	Returns WebLogic Server CPU utilization statistics.
ServerHealthState	Returns the health state of a WebLogic Server.
ServerJVMHeap	Returns statistics on the JVM Heap.
ServerRequests	Returns statistics on the requests received by the WebLogic Server.
ServerSecurity	Monitors statistics on the number of users locked out because invalid usernames and/or passwords were supplied at login.
ServerSockets	Monitors the number of open sockets on a WebLogic Server.
ServerState	Monitors the state (`RUNNING` or not) of a WebLogic Server as reported by the WebLogic Server.
ServerUptime	Monitors how many hours a WebLogic Server has been running.
StartAdminServer	Starts a specified WebLogic Server as the Administration Server for the domain.
StartServer	Starts a specified WebLogic Server as a Managed Server.
StopServer	Stops a specified WebLogic Server, which can be either an Administration Server or a Managed Server.

Managed Server/Cluster Knowledge Scripts

Run the following Knowledge Scripts on managed servers, the Node Manager, and clusters.

Knowledge Script	What It Does
ClusterMessage	Monitors a server's view of the members of a WebLogic cluster.
StartServerNodeMgr	Starts a WebLogic Server as a Managed Server using the Node Manager.

JDBC Connection Pool Knowledge Scripts

Run the following Knowledge Scripts on JDBC connection pools:

Knowledge Script	What It Does
JDBCAvailableConnections	Monitors the available number of connections in a JDBC Connection Pool.
JDBCClients	Monitors statistics on the clients of a JDBC Connection Pool.
JDBCConnectionCapacity	Monitors the current and maximum capacity of a JDBC Connection Pool.
JDBCConnections	Monitors statistics on the connections in a JDBC Connection Pool.

Java Message System (JMS) Knowledge Scripts

Run the following Knowledge Scripts on the JMS subsystem of a WebLogic Server:

Knowledge Script	What It Does
JMS	Monitors the number of JMS Connections in use and the number of JMS servers deployed by a WebLogic Server.
JMSConnectionsSessions	Returns statistics on the number of sessions for JMS connections.
JMSHealthState	Returns the health state of the JMS subsystem of a WebLogic Server.
JMSServersBytesStored	Returns statistics on the number of bytes stored for the JMS servers.
JMSServersDestinations	Returns statistics on the number of destinations instantiated on the JMS servers.
JMSServersHealthState	Returns the health state of the JMS Servers of a WebLogic Server.
JMSServersMsgsStored	Returns statistics on messages for the JMS servers.
JMSServersSessionPools	Returns statistics on the session pools instantiated on the JMS servers.

Java Virtual Machine (JVM) Knowledge Scripts

Run the following Knowledge Scripts on the JVM:

Knowledge Script	What It Does
JRockitGC	Returns statistics on the last time garbage collection was executed in the server and the total amount of time spent in garbage collection.
JRockitThreads	Returns statistics on the number of daemon threads and the total number of threads within the WebLogic Server.

Java Message System (JMS) Pooled Connection Knowledge Scripts

Run the following Knowledge Scripts to monitor the JMS pooled connections:

Knowledge Script	What It Does
JMSPooledConnAvail	Monitors the number of sessions available, unavailable, and reserved in a JMS Pooled Connection.
JMSPooledConnError	Monitors the sessions leaked and sessions unable to be refreshed in a JMS Pooled Connection.
JMSPooledConnSession	Monitors statistics on the sessions in a JMS Pooled Connection. This script reports on the number of allocated and destroyed sessions, the current and maximum capacity of the pool, and the average number of reserved sessions.
JMSPooledConnWait	Monitors the number of threads waiting on the sessions in a JMS Pooled Connection, and the amount of time the threads wait.

Java Transaction API (JTA) Knowledge Scripts

Run the following Knowledge Scripts on the JTA subsystem of a WebLogic Server:

Knowledge Script	What It Does
JTAActiveTrans	Monitors the current number of transactions in progress on a WebLogic Server.
JTACompletedTrans	Monitors the transactions that have completed on a WebLogic Server since the last sample.
JTAHealthState	Returns the health state of the JTA subsystem of a WebLogic Server.
JTATransRolledBack	Provides statistics on the causes for transaction rollbacks.
TransResources	Returns statistics for the transactional resources of a WebLogic Server.
TransResHealthState	Returns the health state of the transactional resources of a WebLogic Server.
TransResHeuristics	Provides a breakdown of the reasons for heuristic completes for the transactional resources of a WebLogic Server.
TransCateg	Returns statistics for the transaction categories of a WebLogic Server.
TransCategRollBacks	Provides statistics on the reasons why transactions were rolled back for the transaction categories of a WebLogic Server.

Enterprise JavaBeans (EJB) Knowledge Scripts

Run the following Knowledge Scripts on the EJBs on a WebLogic Server:

Knowledge Script	What It Does
EntityEJBCache	Returns statistics on caching for an Entity EJB.
EntityEJBError	Returns statistics on errors generated by an Entity EJB.
EntityEJBPool	Returns the percentage of beans that are idle and in-use for an Entity EJB.
EntityEJBTrans	Returns statistics on transactions for an Entity EJB.
EntityEJBWait	Returns the number of times a client has waited for an Entity EJB and the number of times that clients have timed out waiting for an Entity EJB.

Knowledge Script	What It Does
MsgDrivenEJBError	Monitors errors generated by a message-driven EJB.
MsgDrivenEJBPool	Monitors the number of message-driven EJBs that are in use and the number that are idle.
MsgDrivenEJBTrans	Returns statistics on transactions for a message-driven EJB.
MsgDrivenEJBWait	Returns the number of times a client has waited for a message-driven EJB and the number of times that clients have timed out waiting for a message-driven EJB.
StatefulEJBCache	Returns statistics on the cache for a Stateful EJB.
StatefulEJBTrans	Returns statistics on transactions for a Stateful EJB.
StatefulEJBWait	Returns the number of times a client waited for a bean and the number of times that clients have timed out waiting for a bean for the Stateful EJB.
StatelessEJBError	Monitors errors generated by a Stateless EJB.
StatelessEJBPool	Returns the number and percentage of beans that are idle and in use for a Stateless EJB.
StatelessEJBTrans	Returns statistics on transactions for a Stateless EJB.
StatelessEJBWait	Returns the number of times a client waited for a bean and the number of times that clients have timed out waiting for a bean for the Stateless EJB.

Web Applications and Servlets Knowledge Scripts

Run the following Knowledge Scripts on the Web applications and servlets on a WebLogic Server:

Knowledge Script	What It Does
ServletExecTime	Monitors the execution times and number of times that the servlets of a Web application were invoked.
WebAppSessions	Monitors the current number of sessions of a Web application and the number of sessions that have been run since the last sample.

Connector Connections Knowledge Scripts

Run the following Knowledge Scripts on the Connector connections of a WebLogic Server:

Knowledge Script	What It Does
ConnectorConnCurrent	Monitors statistics on the current number of active and free Connector connections.
ConnectorConnRequests	Returns the number of Connector connections created, destroyed, matched, rejected and recycled since the last sample.

Data-Gathering Knowledge Script

Run the following Knowledge Script to start or stop components that gather data for the Knowledge Scripts:

Knowledge Script	What It Does
NetIQAgent	Starts or stops the NetIQ UNIXagent that helps gather data about WebLogic Servers and their components.

SQL Profiling and Monitoring Knowledge Scripts

Run the following Knowledge Script to monitor individual SQL statements:

Knowledge Script	What It Does
JDBCEnableSQLProfiling	Enables or disables profiling of SQL statements.
JDBCSQLMonitoring	Monitors the SQL statements executed within a JDBC Connection Pool.
JDBCSQLMonitoringTopN	Monitors the SQL statements executed within a JDBC Connection Pool that take the longest amount of time.

WebLogic Server Report Knowledge Scripts

Run the following Knowledge Scripts to generate reports:

Knowledge Script	What It Does
Report_HealthSummary	Generates a report summarizing the health of monitored WebLogic servers.
Report_PerfSummary	Generates a report summarizing the performance of monitored WebLogic servers.

Availability

Use this Knowledge Script to monitor availability of a WebLogic Server. This script verifies that a WebLogic Server is running and can accept requests.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Event severity when WebLogic Server is not responding?	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10.

ClusterMessage

Use this Knowledge Script to monitor a server's view of the members of a WebLogic cluster. This script reports statistics on the multicast message and fragments sent and received by a WebLogic server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Fragments sent threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of fragments sent since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when fragments sent exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Fragments received threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of fragments received since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when fragments received exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Resend requests threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of requests to resend a message since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when resend requests exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Messages lost threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of incoming messages lost since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is -1.
Event severity when messages lost exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Foreign fragments dropped threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of fragments received from a foreign domain or foreign cluster since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when foreign fragments dropped exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

ConnectorConnCurrent

Use this Knowledge Script to monitor the number of active and free connections in a Connector Connection Pool. These statistics provide a view of the Connector Connection Pool from the server's perspective, which will help determine if the capacity of the pool is large enough.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Active connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current number of active connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when active connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak active connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of active connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak active connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Average active connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the average number of active connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when average active connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Free connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current number of free connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when free connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Peak free connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of free connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak free connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Percent of connections in use threshold	Specify a threshold value using an integer greater than or equal to –1 and less than or equal to 100. Use –1 to ignore this threshold. If the percent of connections in use exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when percent of connections in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

ConnectorConnRequests

Use this Knowledge Script to monitor the rate at which a Connector Connection Pool is servicing requests for connections. These statistics provide a view of the Connector Connection Pool from the clients' perspective, which can help determine if the capacity of the pool is large enough.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Connections created threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of connections created since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when connections created exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Connections destroyed threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of connections destroyed since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when connections destroyed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Connections matched threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of times since the last sample that a request for a connection was satisfied via an existing connection exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when connections matched exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Connections rejected threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of times since the last sample that a request for a connection was rejected exceeds this threshold, this Knowledge Script raises an event. The default value is –1.

Description	How to Set It
Event severity when connections rejected exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Connections recycled threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of connections that have been recycled since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when connections recycled exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Connections leaked threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of leaked connections since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when leaked connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

EntityEJBCache

Use this Knowledge Script to monitor statistics for an Entity EJB. This script reports caching statistics for an Entity EJB.

This script may be used to determine a cache hit ratio and how frequently instances of the Entity EJB are being activated and passivated. These values will help determine if the size of the cache is appropriate.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Current beans threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of beans currently in use exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when current beans exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Cache accesses threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of cache accesses since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when cache accesses exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Cache hit ratio threshold	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the cache hit ratio (expressed as a percentage) since the last sample falls below this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when cache hit ratio falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Activations threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of activations since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.

Description	How to Set It
Event severity when activations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Passivations threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of passivations since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when passivations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Cache miss count threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the cache miss count since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when cache miss count exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

EntityEJBError

Use this Knowledge Script to monitor errors generated by an Entity EJB. This script reports error statistics for an Entity EJB.

This script may be used to determine the number of times the Entity EJB was destroyed due to an exception, and the number of failed attempts to retrieve an EJB from the pool. These values will help monitor the Entity EJB if errors occur.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Destroyed bean instances threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of times since the last sample that a bean instance was destroyed due to a thrown exception exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when destroyed bean instances exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Miss count threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of failed attempts to retrieve a bean from the free pool since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when miss count exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

EntityEJBPool

Use this Knowledge Script to monitor for the number or percentage of in-use and idle beans in an Entity EJB pool. These values will help determine if the size of the pool has been set properly.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Beans idle threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of beans that are allocated but idle exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when beans idle exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Beans in use threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of beans in use exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when beans in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Percent of pool in use threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the percentage of available beans in the pool that are in use exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when percent of pool in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

EntityEJBTrans

Use this Knowledge Script to monitor the transaction rates for an Entity EJB. Transactions are rolled back when timeouts or application, system or resource errors occur. The JTATransRolledBack Knowledge Script provides a breakdown of the reasons for rollbacks.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Transactions committed threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions committed since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when transactions committed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions rolled back threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions rolled back since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when transactions rolled back exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions timed out threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions timed out since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when transactions timed out exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

EntityEJBWait

Use this Knowledge Script to monitor the number of times a request had to wait for an EJB and the number of times a request timed out waiting for an EJB. Increasing the cache size may help reduce the number of timeouts.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Times waited threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of times since the last sample that clients have waited for a bean exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when times waited exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Timeouts threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of timeouts since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when timeouts exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

HealthCheck

Use this Knowledge Script to make sure a WebLogic Server is running and is able to service requests. This script performs the following checks:

- Verifies the WebLogic Server is running.
- Verifies the WebLogic Server is able to respond to a request.
- Verifies the WebLogic Server is able to accept connections from clients.

This script may also be used to:

- Restart the WebLogic Server if the script determines it is not running.
- Set response time thresholds for responding to requests and establishing connections.
- Raise events (with user-defined severity levels) if the WebLogic Server is not running, is unable to respond to a request, or is unable to accept connections.

If this script detects that the WebLogic Server is not running, it raises a general event to alert you to the condition but it does not perform additional tests for responding to a request and accepting a connection from a client. Therefore, if the WebLogic Server is not running, the script does not return data or compare the thresholds for the **WebLogic Ping time** and the **Average connection time**, and does not raise events to indicate that a WebLogic Ping or connectivity test failed.

If a WebLogic Server is running but is not able to respond to a request, this Knowledge Script raises an event to indicate the ping request failed, but the script does not return data or compare the thresholds for the **WebLogic Ping time**. Similarly, if a WebLogic Server is running, but is not able to accept a connection from a client, this Knowledge Script raises an event to indicate that the connectivity test failed, but the script does not return data or compare the thresholds for the **Average connection time**.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Event severity when server is not running	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10.

Description	How to Set It
Restart WebLogic Server if not running?	Set to **y** to restart the WebLogic server if it is not running. The default value is n.
Use Node Manager to restart server?	Set to **y** to restart the WebLogic server using Node Manager. The default value is n.
Start Command	Set to the name of the script file that you use to start a WebLogic Server, including any parameters that the script requires. The name of the script must include the complete path for the file.
Start Command Parameters	Specify conditions to apply to the Start Command parameter.
Pass name of server, IP address, port, admin username and password to Start Script?	Set to **y** to pass these parameters to the Start Script. These parameters will be added to the end of the string supplied for Start Script. The default value is n.
Start time limit	Set to the number of seconds within which the WebLogic Server should complete initialization. The default value is 300.
Requests	Set to the number of requests, between 1 and 10, that should be made to the server to determine if it is able to respond to requests. The default value is 3.
WebLogic Ping time threshold in secs	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the WebLogic Ping time in seconds exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when WebLogic Ping response not received	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10.
Event severity when WebLogic Ping time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Connections	Set to the number of connections, between 1 and 10, that should be made to the server to determine if it is able to accept connections from clients. The default value is 3.
Average connection time threshold in secs	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the average time in seconds it took the server to establish a connection exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when connection not established	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10.
Event severity when connection time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JDBCAvailableConnections

Use this Knowledge Script to monitor the available number of connections in a JDBC Connection Pool. This script reports the number of available and unavailable connections for a JDBC Connection Pool.

This script may be used to monitor the number available and unavailable connections in a JDBC Connection Pool, and the peak number of available and unavailable connections in a JDBC Connection Pool. These values will help determine if the JDBC Connection Pool is over-utilized or under-utilized.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Available connections threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of available connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when available connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak number of available connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of available connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak number of available connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Unavailable connections threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of unavailable connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when unavailable connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Peak number of unavailable connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of unavailable connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak number of unavailable connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JDBCClients

Use this Knowledge Script to monitor the number of requests that had to wait for a JDBC Connection and how long it took for a request to get a connection. If these values are consistently high, consider increasing the size of the pool.

This script may be used to measure how quickly and efficiently the JDBC Connection Pool is servicing clients' requests and will help determine if the capacity of the pool is sufficient.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Clients waiting threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of clients waiting for a JDBC connection exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when clients waiting exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak clients waiting threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of clients waiting for a JDBC connection exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when peak clients waiting exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak wait time threshold in secs	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the longest time (in seconds) that a client waited for a JDBC connection exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak wait time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Average connection delay time threshold in secs	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the average time (in seconds) that a client waited for a JDBC connection exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when average connection delay time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JDBCConnections

Use this Knowledge Script to monitor a JDBC Connection Pool. This script reports the number of active connections in the JDBC Connection Pool and will indicate whether the capacity of the pool needs adjustment.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Active connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of active connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when active connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Total connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the total number of connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when total connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak active connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of active connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak active connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Percent of connections in use threshold	Specify a threshold value using an integer greater than or equal to –1 and less than or equal to 100. Use –1 to ignore this threshold. If the percent of connections in use exceeds this threshold, this Knowledge Script raises an event. The default value is -1.

Description	How to Set It
Event severity when percent of connections in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Leaked connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of leaked connections since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when leaked connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Refresh failures threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of refresh failures since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when refresh failures exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Average active connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the average number of active connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when average active connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JDBCConnectionCapacity

Use this Knowledge Script to monitor the current and maximum capacity of a JDBC Connection Pool. These values will help determine if the JDBC Connection Pool is too large or too small.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Current capacity threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the current capacity exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when current capacity exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Maximum capacity threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the maximum capacity exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when maximum capacity exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JDBCEnableSQLProfiling

Use this Knowledge Script to enable or disable profiling of SQL statements. This script provides a way to enable or disable SQL statement profiling without using the Administrator Console.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Run once.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Enable SQL statement profiling	Set to **y** to enable SQL statement profiling within the WebLogic Server. The default value is y.

JDBCSQLMonitoring

Use this Knowledge Script to monitor the SQL statements executed within a JDBC Connection Pool. These values will help determine if the JDBC Connection Pool is configured properly or has a slow response time, or if the database the pool connects to has a slow response time.

Version of WebLogic Supported

8.1 SP6

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
SQL statement filter	Set to a string that specifies the SQL statement filter. The SQL statement filter matches substrings of the SQL statement text. The default value is .*.
Number of statements executed threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of SQL statements executed since the last sample exceeds this threshold, an event is raised. The default value is –1.
Event severity when number of statements executed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Average statement execution time threshold in secs	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the average statement execution time in seconds since the last sample exceeds this threshold, an event is raised. The default value is –1.
Event severity when average statement execution time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Minimum statement execution time threshold in secs	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the minimum statement execution time in seconds since the last sample exceeds this threshold, an event is raised. The default value is –1.
Event severity when minimum statement execution time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Maximum statement execution time threshold in secs	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the maximum statement execution time in seconds since the last sample exceeds this threshold, an event is raised. The default value is –1.
Event severity when maximum statement execution time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JDBCSQLMonitoringTopN

Use this Knowledge Script to monitor the SQL statements executed within a JDBC Connection Pool that take the longest amount of time. These values will help determine which calls to the database are most adversely affecting performance.

Version of WebLogic Supported

8.1 SP6

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
SQL statement filter	Set to a string that specifies the SQL statement filter. The SQL statement filter matches substrings of the SQL statement text.
Number of statements	Specify the number of statements, between 1 and 5, for which data should be collected. The default value is 5.
Execution time threshold in secs	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the execution time of a SQL statement in seconds exceeds this threshold, an event is raised. The default value is –1.
Event severity when execution time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JMS

Use this Knowledge Script to monitor the Java Message System (JMS). This script monitors the number of JMS Connections in use and the number of JMS servers deployed by a WebLogic Server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Current connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current number of JMS Connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when current connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak connections threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of JMS Connections exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak connections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Connections made threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of JMS Connections made to this WebLogic Server since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when connections made exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Current servers threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current number of deployed JMS Servers exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when current servers exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Peak servers threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of deployed JMS Servers exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak servers exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Servers deployed threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of JMS Servers deployed since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when servers deployed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JMSConnectionsSessions

Use this Knowledge Script to monitor JMS connections. This script monitors the number of sessions in use for each JMS Connection and the rate at which sessions are being opened.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Current sessions threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current number of sessions for the JMS Connection exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when current sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak sessions threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of sessions for the JMS Connection exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Sessions opened threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of sessions opened for the JMS Connection since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when sessions opened exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JMSHealthState

Use this Knowledge Script to monitor the health state of the JMS subsystem of a WebLogic Server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Scale to 100?	Set to **y** to scale the values to 100. The default values range from 0-3, where 0 is `OK`, and 3 is `FAIL`. Setting to y will scale the values from 0-100, where 0 is `FAIL` and 100 is `OK`. The default value is n.
Event for health state of FAIL?	Set to **y** to raise an event if the health state is `FAIL`. The default value is y.
Event severity when health state is FAIL?	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5.
Event for health state of CRITICAL?	Set to **y** to raise an event if the health state is `CRITICAL`. The default value is y.
Event severity when health state is CRITICAL	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15.
Event for health state of WARNING?	Set to **y** to raise an event if the health state is `WARNING`. The default value is y.
Event severity when health state is WARNING	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Event for health state of OK?	Set to **y** to raise an event if the health state is `OK`. The default value is n.
Event severity when health state is OK	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 35.

JMSPooledConnAvail

Use this Knowledge Script to monitor number of sessions available, unavailable, and reserved in a JMS Pooled Connection. These values will help determine if the JMS Pooled Connection is too large or too small.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Available sessions threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of available sessions exceeds this threshold, an event is raised. The default value is –1.
Event severity when available sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak available sessions threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of available sessions exceeds this threshold, an event is raised. The default value is –1.
Event severity when peak available sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Reserved sessions threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of reserved sessions exceeds this threshold, an event is raised. The default value is –1.
Event severity when reserved sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak reserved sessions threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of reserved sessions exceeds this threshold, an event is raised. The default value is –1.
Event severity when peak reserved sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Unavailable sessions threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of unavailable sessions exceeds this threshold, an event is raised. The default value is –1.

Description	How to Set It
Event severity when unavailable sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak number of unavailable sessions threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of unavailable sessions exceeds this threshold, an event is raised. The default value is –1.
Event severity when peak number of unavailable sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JMSPooledConnError

Use this Knowledge Script to monitor the sessions leaked and sessions unable to be refreshed in a JMS Pooled Connection. These values will help determine when errors and leaks occur when using a JMS Pooled Connection.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Leaked sessions threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of leaked sessions since the last sample exceeds this threshold, an event is raised. The default value is 0.
Event severity when leaked sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Refresh failures threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of refresh failures since the last sample exceeds this threshold, an event is raised. The default value is 0.
Event severity when refresh failures exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JMSPooledConnSession

Use this Knowledge Script to monitor statistics on the sessions in a JMS Pooled Connection. This script reports on the number of allocated and destroyed sessions, the current and maximum capacity of the pool, and the average number of reserved sessions. These values will help determine if the JMS Pooled Connection is overloaded or under-utilized.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Current capacity threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of current capacity exceeds this threshold, an event is raised. The default value is –1.
Event severity when current capacity exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Maximum capacity threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the maximum capacity of available sessions exceeds this threshold, an event is raised. The default value is –1.
Event severity when maximum capacity exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Allocated sessions threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of allocated sessions since the last sample exceeds this threshold, an event is raised. The default value is –1.
Event severity when allocated sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Destroyed sessions threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of destroyed sessions since the last sample exceeds this threshold, an event is raised. The default value is –1.
Event severity when destroyed sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Average number of reserved sessions threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the average number of reserved sessions exceeds this threshold, an event is raised. The default value is –1.
Event severity when average number of reserved sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JMSPooledConnWait

Use this Knowledge Script to monitor the number of threads waiting on the sessions in a JMS Pooled Connection, and the amount of time the threads wait. These values will help determine if the JMS Pooled Connection is overloaded.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Threads waiting threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of threads waiting for a session exceeds this threshold, an event is raised. The default value is –1.
Event severity when threads waiting exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak number of threads waiting threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of threads waiting for a session exceeds this threshold, an event is raised. The default value is –1.
Event severity when peak number of threads waiting exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak wait time threshold in secs	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the longest amount of time a thread waited for a session in seconds since the last sample exceeds this threshold, an event is raised. The default value is –1.
Event severity when peak wait time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Average creation delay time threshold in secs	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the average amount of time to create each session in seconds exceeds this threshold, an event is raised. The default value is –1.
Event severity when average creation delay time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JMSServersBytesStored

Use this Knowledge Script to monitor JMS servers. This script monitors the number of bytes consumed by messages on each JMS server.

The **Time in threshold condition** parameter is the time (in seconds) that the current number of bytes consumed exceeds a WebLogic Server threshold for that JMS server. This value, along with the current number of bytes, can help you adjust the maximum bytes for the JMS server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Current bytes threshold	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the current number of bytes stored on this JMS Server exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when current bytes exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Pending bytes threshold	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the current number of pending bytes stored on this JMS server exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when pending bytes exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak bytes threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of bytes stored on this JMS Server exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak bytes exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Time in threshold condition threshold in secs	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the number of seconds spent in the threshold condition (due to the number of bytes stored on this JMS Server) since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when time in threshold condition exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JMSServersDestinations

Use this Knowledge Script to monitor JMS servers. This script monitors the current number of destinations for each JMS server and the rate at which those destinations are being created.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Current destinations threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current number of destinations for this JMS server exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when current destinations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak destinations threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of destinations for this JMS server exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak destinations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Destinations instantiated threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of destinations instantiated on this JMS server since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when destinations instantiated exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JMSServersHealthState

Use this Knowledge Script to monitor the health state of the JMS servers of a WebLogic Server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Scale to 100?	Set to y to scale the values to 100. The default values range from 0-3, where 0 is `OK`, and 3 is `FAIL`. Setting to y will scale the values from 0-100, where 0 is `FAIL` and 100 is `OK`. The default value is n.
Event for health state of FAIL?	Set to **y** to raise an event if the health state is `FAIL`. The default value is y.
Event severity when health state is FAIL?	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5.
Event for health state of CRITICAL?	Set to **y** to raise an event if the health state is `CRITICAL`. The default value is y.
Event severity when health state is CRITICAL	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15.
Event for health state of WARNING?	Set to **y** to raise an event if the health state is `WARNING`. The default value is y.
Event severity when health state is WARNING	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Event for health state of OK?	Set to **y** to raise an event if the health state is `OK`. The default value is n.
Event severity when health state is OK	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 35.

JMSServersMsgsStored

Use this Knowledge Script to monitor JMS servers. This script monitors the number of messages on each JMS server. The time in threshold condition is the number of seconds in which the current number of messages is above or below a WebLogic Server threshold for that JMS server. This value, along with the current number of messages, can help you adjust the maximum messages for the JMS server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Current messages threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current number of messages stored on this JMS server, not including pending messages, exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when current messages exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Pending messages threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current number of pending messages (unacknowledged or uncommitted) stored on this JMS server exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when pending messages exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak messages threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of messages stored on this JMS Server exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak messages exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Time in threshold condition threshold in secs	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the number of seconds time spent in the threshold condition (due to the number of messages stored on this JMS server) exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when time in threshold condition exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JMSServersSessionPools

Use this Knowledge Script to monitor JMS servers. This script monitors the number of session pools in use by each JMS server and the rate at which those pools are being created.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Current session pools threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current number of session pools instantiated on this JMS server exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when current session pools exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak session pools threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of session pools instantiated on this JMS server exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak session pools exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Session pools instantiated threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of session pools instantiated on this JMS server since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when session pools instantiated bytes exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JRockitGC

Use this Knowledge Script to monitor the last time garbage collection was executed in the server and the total amount of time spent in garbage collection. These values will help determine potential bottlenecks within the WebLogic Server instance.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Seconds since last garbage collection ended threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of seconds since the last garbage collection run exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when seconds since last garbage collection exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Number of garbage collection runs threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of garbage collection runs since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when number of garbage collection runs exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Average garbage collection time threshold in secs	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the average time spent in a garbage collection run in seconds since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when average garbage collection time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JRockitThreads

Use this Knowledge Script to monitor the number of daemon threads and the total number of threads within the WebLogic Server. These values will help determine potential bottlenecks within the WebLogic Server instance.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Number of daemon threads threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of daemon threads exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when number of daemon threads exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Total number of threads threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the total number of threads exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when total number of threads exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JTAActiveTrans

Use this Knowledge Script to monitor the current number of transactions in progress on a WebLogic Server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Active transactions threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of active transactions exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when active transactions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JTACompletedTrans

Use this Knowledge Script to monitor the Java Transaction API (JTA). This script monitors the transactions that have completed on a WebLogic Server since the last sample. Transactions are rolled back when timeouts or application, system or resource errors occur. The JTATransRolledBack script provides a breakdown of the reasons for rollbacks.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Total transactions threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the total number of transactions since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when total transactions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions committed threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions committed since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when transactions committed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions rolled back threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions rolled back since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when transactions rolled back exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Heuristic completes threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions with heuristic completes since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.

Description	How to Set It
Event severity when heuristic completes exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Average commit time threshold in secs	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the average commit time in seconds exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when average commit time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions abandoned threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions abandoned since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is -1.
Event severity when transactions abandoned exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

JTAHealthState

Use this Knowledge Script to monitor the health state of the JTA subsystem of a WebLogic Server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Scale to 100?	Set to y to scale the values to 100. The default values range from 0-3, where 0 is `OK`, and 3 is `FAIL`. Setting to y will scale the values from 0-100, where 0 is `FAIL` and 100 is `OK`. The default value is n.
Event for health state of FAIL?	Set to **y** to raise an event if the health state is `FAIL`. The default value is y.
Event severity when health state is FAIL?	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5.
Event for health state of CRITICAL?	Set to **y** to raise an event if the health state is `CRITICAL`. The default value is y.
Event severity when health state is CRITICAL	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15.
Event for health state of WARNING?	Set to **y** to raise an event if the health state is `WARNING`. The default value is y.
Event severity when health state is WARNING	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Event for health state of OK?	Set to **y** to raise an event if the health state is `OK`. The default value is n.
Event severity when health state is OK	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 35.

JTATransRolledBack

Use this Knowledge Script to obtain a breakdown of the reasons why transactions were rolled back.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Timeouts threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of rollbacks due to timeouts since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when timeouts exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Resource errors threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of rollbacks due to resource errors since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when resource errors exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Application errors threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of rollbacks due to application errors since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when application errors exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
System errors threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of rollbacks due to system errors since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when system errors exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

LogAccessLog

Use this Knowledge Script to monitor entries that are added to the Web server log of a WebLogic Server. The entries that are monitored can be restricted by supplying Perl regular expressions to indicate which entries should be included or excluded from consideration. The script checks only the new log entries that were created since the last time the script examined the log. By monitoring `access.log`, you can gather statistics on HTTP requests and sessions.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Number matched threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of log entries that matched the search criteria exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when number matched exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Include filter	Set to a string that is a regular expression that specifies the include filter.
Include modifier	Set to a string that is a modifier for the regular expression include filter. The default value is a null string.
Exclude filter	Set to a string that is a regular expression that specifies the exclude filter. The default value is a null string.
Exclude modifier	Set to a string that is a modifier for the regular expression exclude filter. The default value is a null string.

LogAccessLogSetPath

Use this Knowledge Script to set the absolute pathname for a Web server log file. The LogAccessLog Knowledge Script needs an absolute pathname for the log file, but the Administration Console of WebLogic Server will accept relative pathnames. This script provides a way to set the absolute path without having to do it through the Administration Console.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Absolute path name for access.log file	The absolute pathname of the log file for the Web server.

LogWebLogic

Use this Knowledge Script to monitor entries that are added to the log for a WebLogic Server. The entries that are monitored can be restricted by supplying Perl regular expressions that indicate which entries should be included or excluded from consideration. The script checks only the new log entries that were created since the last time the script examined the log.

Note
If you are running WebLogic Server 8.1, you must specify an absolute path to the WebLogic log file in order to run the LogWebLogic Knowledge Script successfully. If the LogWebLogic script is run and you have not set an absolute path, you receive the following event message: 'Absolute pathname for log file required'. Use the LogWebLogicSetPathKnowledge Script to specify the absolute path to the WebLogic log file. You will continue to receive an event message until you reboot the WebLogic 8.1 server where the log file resides.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Number matched threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of log entries that matched the search criteria exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when number matched exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Include filter	Set to a string that is a regular expression that specifies the include filter. The default value is (*).
Include modifier	Set to a string that is a modifier for the regular expression include filter. The default value is a null string.

Description	How to Set It
Exclude filter	Set to a string that is a regular expression that specifies the exclude filter. The default value is a null string.
Exclude modifier	Set to a string that is a modifier for the regular expression exclude filter. The default value is a null string.

LogWebLogicSetPath

Use this Knowledge Script to set the absolute pathname for a WebLogic Server log file. The LogWebLogic Knowledge Script needs an absolute pathname for the log file, but the Administration Console of WebLogic Server will accept relative pathnames. This script provides a way to set the absolute path without having to do it through the Administration Console.

Notes

If you are running BEA WebLogic Server 8.1, you must specify an absolute path to the WebLogic log file in order to run the LogWebLogic Knowledge Script successfully. If you try to run the LogWebLogic Knowledge Script without first setting an absolute path, you receive the following event message: 'Absolute pathname for log file required'.

Use the LogWebLogicSetPath Knowledge Script to specify the absolute path to the WebLogic log file. You will continue to receive an event message until you reboot the WebLogic 8.1 server where the log file resides.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Absolute path name for WebLogic Server log file	The absolute pathname of the WebLogic Server's log file.

Memory

Use this Knowledge Script to monitor the physical and virtual memory use of a WebLogic Server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Real memory size threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the real memory size of a WebLogic Server in kilobytes exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when real memory size exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Virtual memory size threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the virtual memory size of a WebLogic Server in kilobytes exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when virtual memory size exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Percent of real memory in use threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the percent of real memory in use of a WebLogic Server in kilobytes exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when percent of real memory in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

MsgDrivenEJBError

Use this Knowledge Script to monitor errors generated by a message-driven EJB. This script reports error statistics for a message-driven EJB.

This script may be used to determine the number of times the message-driven EJB was destroyed due to an exception, and the number of failed attempts to retrieve an EJB from the pool. These values will help monitor the message-driven EJB if errors occur.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Destroyed bean instances threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of times since the last sample that a bean instance was destroyed due to a thrown exception exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when destroyed bean instances exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Miss count threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of failed attempts to retrieve a bean from the free pool since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when miss count exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

MsgDrivenEJBPool

Use this Knowledge Script to monitor for the number or percentage of beans that are in use and idle in a message-driven EJB pool. These values will help determine if the size of the pool has been set properly.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Beans idle threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of beans that are allocated but idle exceeds this threshold, this Knowledge Script raises an event. The default value is -1.
Event severity when beans idle exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Beans in use threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of beans in use exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when beans in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Percent of pool in use threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the percent of beans available in the pool in use exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when percent of pool in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

MsgDrivenEJBTrans

Use this Knowledge Script to monitor a message-driven EJB. This script monitors the transaction rates for a message-driven EJB. Transactions are rolled back when timeouts or application, system or resource errors occur. The JTATransRolledBack Knowledge Script provides a breakdown of the reasons for rollbacks.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Transactions committed threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions committed since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when transactions committed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions rolled back threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions rolled back since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when transactions rolled back exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions timed out threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions timed out since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when transactions timed out exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

MsgDrivenEJBWait

Use this Knowledge Script to monitor a message-driven EJB. This script monitors the number of times a request had to wait for an EJB and the number of times a request timed out waiting for an EJB. Increasing the cache size may help reduce the number of timeouts.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Times waited threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of times since the last sample that clients have waited for a bean exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when times waited exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Timeouts threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of timeouts since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when timeouts exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

NetIQAgent

Use this Knowledge Script to stop (and start) the NetIQ agent, which most of the scripts use to gather information from WebLogic servers.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Event severity when NetIQ WebLogic agent cannot be started	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10.
Event severity when NetIQ WebLogic agent cannot be stopped	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15.
Event severity when NetIQ WebLogic agent is started	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Event severity when NetIQ WebLogic agent is stopped	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Enable?	Set to **y** to start the NetIQ agent; set to n to stop it. The default value is y.

Report_HealthSummary

Use this Report Knowledge Script to generate a report summarizing the health of monitored WebLogic servers. The report provides data gathered by the HealthCheck Knowledge Script.

Resource Object

AppManager repository.

Default Schedule

The default schedule for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse (...)** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse (...)** button to select the days of the week to include in your report.
Aggregation by	Select the time period (Hour, Minute, or Day) by which the data in your report is aggregated.
Aggregation interval	Select the interval between aggregations of the data in your report. This parameter uses the time period specified in the **Aggregation by** parameter to calculate the interval.
Report Component Selection	Use the following parameters to define which data and statistics are displayed in the report.
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default value is y.
Include Running detail table?	Set to **y** to include data from the Availability detail table in the report. The default value is y.
Include Running chart?	Set to **y** to include data from the Availability chart in the report. The default value is y.
Threshold on running chart	Specify an integer to set a threshold for the Availability chart. Use -1 to ignore this threshold.
Include WebLogic Ping Response Time detail table?	Set to **y** to include data from the WebLogic Ping Response Time detail table in the report. The default value is y.
Include WebLogic Ping Response Time chart?	Set to **y** to include data from the WebLogic Ping Response Time chart in the report. The default value is y.

Description	How to Set It
Units for WebLogic Ping Response Time report	Select the measurement units to be used in the WebLogic Ping Response Time report. The default value is msec (milliseconds).
Threshold on WebLogic Ping Response Time chart	Specify an integer to set a threshold for the WebLogic Ping Response Time chart. Use -1 to ignore this threshold. The default value is 0.
Include WebLogic Connect Time detail table?	Set to **y** to include data from the WebLogic Connect Time detail table in the report. The default value is y.
Include WebLogic Connect Time chart?	Set to **y** to include data from the WebLogic Connect Time chart in the report. The default value is y.
Units for WebLogic Connect Time report	Select the measurement units to be used in the WebLogic Connect Time report. The default value is msec (milliseconds).
Threshold on WebLogic Connect Time chart	Specify an integer to set a threshold for the WebLogic Connect Time chart. Use -1 to ignore this threshold. The default value is 0.
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Customize chart appearance	Click the **Browse (...)** button to open the Chart Settings window. Define the graphic properties of the charts in your report. The default value is Ribbon.
Select report location	Click the **Browse (...)** button to open the Publishing Options window. Define the report filename and specify a default folder this report. The default value is WebLogicSvr_HealthSummary
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default value is n.
Index-Report Title	Click in the Value column, and click the **Browse (...)** button to open the Report Properties window. Set the properties parameters as desired The default title is WebLogicSvr_HealthSummary.
Add time stamp to title?	Set to y to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default value is n.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Generate event on success?	Set to **y** to raise an event when the report is successfully generated. The default value is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red level indicator).

Report_PerfSummary

Use this Report Knowledge Script to generate a report summarizing the throughput performance of monitored WebLogic servers. The report provides data from the ServerCPU and ServerRequests Knowledge Scripts.

Resource Object

AppManager repository.

Default Schedule

The default schedule for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	Use the following parameters to select the data for your report.
Select computer(s)	Click the **Browse [...]** button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the **Browse (...)** button to open the time browser. Set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click the **Browse (...)** button to select the days of the week to include in your report.
Aggregation by	Select the time period (Hour, Minute, or Day) by which the data in your report is aggregated.
Aggregation interval	Select the interval between aggregations of the data in your report. This parameter uses the time period specified in the “Aggregation by” parameter to calculate the interval.
Report Component Selection	Use the following parameters to define which data and statistics are displayed in the report.
Include parameter card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default value is y.
Include CPU Utilization detail table?	Set to **y** to include data from the CPU Utilization detail table in the report. The default value is y.
Include CPU Utilization chart?	Set to **y** to include data from the CPU Utilization chart in the report. The default value is y.
Threshold on CPU Utilization chart?	Specify an integer to set a threshold for the CPU Utilization chart. Use -1 to ignore this threshold. The default value is 0.
Include Throughput detail table?	Set to **y** to include data from the Throughput detail table in the report. The default value is y.
Include Throughput chart?	Set to **y** to include data from the Throughput chart in the report. The default value is y.
Threshold on Throughput chart	Specify an integer to set a threshold for the Throughput chart. Use -1 to ignore this threshold. The default value is 0.

Description	How to Set It
Report settings	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Customize chart appearance	Click the **Browse (...)** button to open the Chart Settings window. Define the graphic properties of the charts in your report. The default value is Ribbon.
Select report location	Click the **Browse (...)** button to open the Publishing Options window. Define the report filename and specify a default folder this report. The default value is WebLogicSvr_PerfSummary.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report. The default value is n.
Index-Report Title	Click in the Value column, and click the **Browse (...)** button to open the Report Properties window. Set the properties parameters as desired. The default title is WebLogicSvr_Perf Summary.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output. The default value is n.
Event notification	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Generate event on success?	Set to **y** to raise an event when the report is successfully generated. The default value is y.
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 35 (magenta level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25 (blue level indicator).
Severity level for report failure.	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red level indicator).

SecurityUserLockout

Use this Knowledge Script to monitor statistics on the number of users locked out because invalid usernames and/or passwords were supplied at login.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
User lockouts threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of user lockouts since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when user lockouts exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Invalid logins threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of invalid logins since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when invalid logins exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Invalid logins while user locked out threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of invalid logins while a user was locked out since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when invalid logins while user locked out exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
User unlocks threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of times since the last sample that a user was unlocked exceeds this threshold, this Knowledge Script raises an event. The default value is –1.

Description	How to Set It
Event severity when user unlocks exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Locked users threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current number of locked users exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when locked users exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

ServerCPU

Use this Knowledge Script to monitor the utilization of a WebLogic Server. This script monitors the amount of CPU the server is consuming.

This script may be used to track how busy a server is at a given time.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
CPU usage threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the CPU utilization for the WebLogic Server exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

ServerHealthState

Use this Knowledge Script to monitor the health state of a WebLogic Server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Scale to 100?	Set to **y** to scale the values to 100. The default values range from 0-3, where 0 is `OK`, and 3 is `FAIL`. Setting to y will scale the values from 0-100, where 0 is `FAIL` and 100 is `OK`. The default value is n.
Event for health state of FAIL?	Set to **y** to raise an event if the health state is `FAIL`. The default value is y.
Event severity when health state is FAIL?	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5.
Event for health state of CRITICAL?	Set to **y** to raise an event if the health state is `CRITICAL`. The default value is y.
Event severity when health state is CRITICAL	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15.
Event for health state of WARNING?	Set to **y** to raise an event if the health state is `WARNING`. The default value is y.
Event severity when health state is WARNING	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Event for health state of OK?	Set to **y** to raise an event if the health state is `OK`. The default value is n.
Event severity when health state is OK	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 35.

ServerJVMHeap

Use this Knowledge Script to monitor the utilization of a WebLogic Server. This script monitors the percentage of a WebLogic server's JVM heap that is currently used. If this value is consistently near 100%, consider increasing the size of the WebLogic server's JVM heap.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Heap size threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current size of the heap in KB exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when heap size exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Free heap threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of KB available in the heap falls below this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when free heap falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Percent heap used threshold	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the percentage of the JVM Heap that is currently used exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when percent heap used exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

ServerRequests

Use this Knowledge Script to monitor the utilization and throughput of a WebLogic Server. This script monitors the server's Execute Queue.

This script may be used to track how busy a server is at a given time.

Note
If the number of requests waiting on the Execute Queue is 0, the value for the "Oldest request" on the queue is not returned and the threshold comparison is not performed.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Throughput threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of requests the WebLogic Server has serviced since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when throughput exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Waiting requests threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of requests waiting on the Execute Queue exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when waiting requests exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Oldest request threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of seconds the oldest request has been on the Execute Queue exceeds this threshold, this Knowledge Script raises an event. The default value is –1.

Description	How to Set It
Event severity when oldest request exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Idle threads threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of idle threads in the Execute Queue exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when idle threads exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Percent threads in use threshold	Specify a threshold value using an integer greater than or equal to –1 and less than or equal to 100. Use –1 to ignore this threshold. If the percent of threads in the Execute Queue exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when percent threads in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

ServerSecurity

Use this Knowledge Script to monitor statistics on the number of users locked out because invalid usernames and/or passwords were supplied at login.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
User lockouts threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of user lockouts since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when user lockouts exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Invalid logins threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of invalid logins since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when invalid logins exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Invalid logins while user locked out threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of invalid logins while a user was locked out since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when invalid logins while user locked out exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
User unlocks threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of times since the last sample that a user was unlocked exceeds this threshold, this Knowledge Script raises an event. The default value is –1.

Description	How to Set It
Event severity when user unlocks exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Locked users threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current number of locked users exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when locked users exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

ServerSockets

Use this Knowledge Script to monitor the number of sockets a WebLogic Server has open.

This script may be used to track the number of server connections and how busy a WebLogic Server is.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Sockets currently open threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of sockets currently open exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when sockets currently open exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Total sockets opened threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of sockets opened since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when total sockets opened exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

ServerState

Use this Knowledge Script to monitor the state of a WebLogic Server as reported by the WebLogic Server. If the state is anything other than `RUNNING`, the server may not be responding properly.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Event for any state other than `RUNNING`?	Set to **y** to raise an event if the health state is not `RUNNING`. The default value is y.
Event severity when health state is not `RUNNING`?	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5.
Event for state of `RUNNING`?	Set to **y** to raise an event if the state is `RUNNING`. The default value is n.
Event severity when state is `RUNNING`	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 35.

ServerUptime

Use this Knowledge Script to monitor how many hours a WebLogic Server has been running.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Maximum server up time threshold	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the overall average execution time (in seconds) of the servlet exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Event severity when server has restarted	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

ServletExecTime

Use this Knowledge Script to monitor the execution times and number of times that the servlets of a Web application were invoked. The short-term average is the average execution time since the last sample; the long-term average is the average execution time since the WebLogic server was started.

The overall average execution time of a servlet is calculated as the total time that the servlet has run since the WebLogic server was started, divided by the total number of times the servlet was invoked since the WebLogic server was started. This average will not tend to change very much if the WebLogic server has been running for a long time.

The short-term average execution time of a servlet is calculated as the time that the servlet has run since the last sample, divided by the number of times the servlets was invoked since the last sample. This average gives a better impression of how well the servlet has been performing since the last sample.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Overall average threshold in secs	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the overall average execution time (in seconds) of the servlet exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when overall average exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Short term average threshold in secs	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the short-term average execution time (in seconds) of the servlet exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when short-term average exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Longest time threshold in secs	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the longest execution time (in seconds) of the servlet exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when longest time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Shortest time threshold	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the shortest execution time (in seconds) of the servlet exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when shortest time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Invocations threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of invocations of the servlet since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when invocations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Reloads threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of reloads of the servlet since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when reloads exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

StartAdminServer

Use this Knowledge Script to start a WebLogic Server as the Administration Server for a domain.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Event severity when script fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10.
Event severity when server cannot be started	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10.
Event severity when server is started	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Start	Enter the name (with the full path) of the script that you use to start an Administration Server. The default value is blank (no default). This is a mandatory field.
Start Script Parameters	Enter the parameters for the start script, if any.
Restart server if already running? (y/n)	Set to **y** to restart the server if it is already running. The default value is y.
Pass name of server, IP address, port, admin username and password to Start Script?	Set to **y** to pass these parameters to the Start Script. These parameters will be added to the end of the string supplied for Start Script. The default value is n.
Start time limit	Set to the number of seconds within which the WebLogic Server should complete initialization. The default value is 300.

StartServer

Use this Knowledge Script to start a managed WebLogic Server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Event severity when server cannot be started	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10.
Event severity when server is started	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Start	Set to the name of the script that you use to start an Administration Server. The default value is blank (no default).
Start Script Parameters	Enter the parameters for the start script, if any.
Restart server if already running?	Set to **y** to restart the server if it is already running. The default value is y.
Pass name of server, IP address, port, admin username and password to Start Script?	Set to **y** to pass these parameters to the Start Script. These parameters will be added to the end of the string supplied for Start Script. The default value is n.
Start time limit	Set to the number of seconds within which the WebLogic Server should complete initialization. The default value is 300.

StartServerNodeMgr

Use this Knowledge Script to start WebLogic Server as a Managed Server using the Node Manager.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Event severity when server cannot be started	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10.
Event severity when server is started	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Restart server if already running?	Set to **y** to restart the server if it is already running. The default value is y.

StatefulEJBCache

Use this Knowledge Script to monitor statistics for a Stateful EJB. This script reports caching statistics for a Stateful EJB.

This script may be used to determine a cache hit ratio and how frequently instances of the Stateful EJB are rendered active or passive. These values will help determine if the size of the cache is appropriate.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Current beans threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of beans currently in use exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when current beans exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Cache accesses threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of cache accesses since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when cache accesses exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Cache hit ratio threshold	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the cache hit ratio (expressed as a percentage) since the last sample falls below this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when cache hit ratio falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Activations threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of activations since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.

Description	How to Set It
Event severity when activations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Passivations threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of passivations since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when passivations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Cache miss count threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the cache miss count since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when cache miss count exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

StatefulEJBTrans

Use this Knowledge Script to monitor Stateful EJBs. This script monitors the transaction rates for a Stateful EJB. Transactions are rolled back when timeouts or application, system, or resource errors occur. The JTATransRolledBack Knowledge Script provides a breakdown of the reasons for rollbacks.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Transactions committed threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions committed since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when transactions committed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions rolled back threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions rolled back since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when transactions rolled back exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions timed out threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions timed out since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when transactions timed out exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

StatefulEJBWait

Use this Knowledge Script to monitor Stateful EJBs. This script monitors the number of times a request had to wait for an EJB and the number of times a request timed out waiting for an EJB. Increasing the cache size may help reduce the number of timeouts.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Times waited threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of times since the last sample that clients have waited for a bean exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when times waited exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Timeouts threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of timeouts since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when timeouts exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

StatelessEJBError

Use this Knowledge Script to monitor errors generated by a Stateless EJB. This script reports error statistics for a Stateless EJB.

This script may be used to determine the number of times the Stateless EJB was destroyed due to an exception, and the number of failed attempts to retrieve an EJB from the pool. These values will help monitor the Stateless EJB if errors occur.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Destroyed bean instances threshold	Specify a threshold value using an integer value greater than or equal to –1. Use –1 to ignore this threshold. If the number of times since the last sample that a bean instance was destroyed due to a thrown exception exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when destroyed bean instances exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Miss count threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of failed attempts to retrieve a bean from the free pool since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when miss count exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

StatelessEJBPool

Use this Knowledge Script to monitor for the number or percentage of in-use and idle beans in a Stateless EJB pool. These values will help determine if the size of the pool has been set properly.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Beans idle threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of beans that are allocated but idle exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when beans idle exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Beans in use threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of beans in use exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when beans in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Percent of pool in use threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the percentage of beans in the pool that are in use exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when percent of pool in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

StatelessEJBTrans

Use this Knowledge Script to monitor Stateless EJBs. This script monitors the transaction rates for a Stateless EJB. Transactions are rolled back when timeouts or application, system or resource errors occur. The JTATransRolledBack Knowledge Script provides a breakdown of the reasons for rollbacks.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Transactions committed threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions committed since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when transactions committed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions rolled back threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions rolled back since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when transactions rolled back exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions timed out threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions timed out since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when transactions timed out exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

StatelessEJBWait

Use this Knowledge Script to monitor Stateless EJBs. This script monitors the number of times a request had to wait for an EJB and the number of times a request timed out waiting for an EJB. Increasing the cache size may help reduce the number of timeouts.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Times waited threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of times since the last sample that clients have waited for a bean exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when times waited exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Timeouts threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of timeouts since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when timeouts exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

StopServer

Use this Knowledge Script to shut down a WebLogic Server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Event severity when unable to stop server	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 10.
Event severity when server is stopped	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

TransCateg

Use this Knowledge Script to monitor statistics for transaction categories. This script monitors the transactions that have completed on a WebLogic Server since the last sample on a per transaction category basis. Transactions are rolled back when timeouts or application, system or resource errors occur. The TransCategRollBacks Knowledge Script provides a breakdown of the reasons for rollbacks.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Transactions completed threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of transactions completed since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is -1.
Event severity when transactions completed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions committed threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions committed since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when transactions committed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions rolled back threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions rolled back since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when transactions rolled back exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Average commit time threshold in secs	Specify a threshold value using a real number greater than or equal to –1. Use –1 to ignore this threshold. If the average commit time in seconds exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when average commit time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Heuristic completes threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of heuristic completes since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when heuristic completes exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions abandoned threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions abandoned since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when transactions abandoned exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

TransCategRollBacks

Use this Knowledge Script to monitor the reasons why transactions were rolled back. This script reports this information on a per transaction category basis.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Timeouts threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of rollbacks due to timeouts since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when timeouts exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Resource errors threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of rollbacks due to resource errors since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when resource errors exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Application errors threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of rollbacks due to application errors since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when application errors exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
System errors threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of rollbacks due to system errors since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when system errors exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

TransResHealthState

Use this Knowledge Script to monitor the health state of the transactional resources of a WebLogic Server.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Scale to 100?	Set to **y** to scale the values to 100. The default values range from 0-3, where 0 is `OK`, and 3 is `FAIL`. Setting to y will scale the values from 0-100, where 0 is `FAIL` and 100 is `OK`. The default value is n.
Event for health state of FAIL?	Set to **y** to raise an event if the health state is `FAIL`. The default value is y.
Event severity when health state is FAIL?	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5.
Event for health state of CRITICAL?	Set to **y** to raise an event if the health state is `CRITICAL`. The default value is y.
Event severity when health state is CRITICAL	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 15.
Event for health state of WARNING?	Set to **y** to raise an event if the health state is `WARNING`. The default value is y.
Event severity when health state is WARNING	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Event for health state of OK?	Set to **y** to raise an event if the health state is `OK`. The default value is n.
Event severity when health state is OK	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 35.

TransResHeuristics

Use this Knowledge Script to monitor the reasons why transactions for transactional resources completed with an heuristic status. This script monitors the transactions that completed with a heuristic status for each of a WebLogic server's transactional resources. Transactions are rolled back when timeouts or application, system or resource errors occur.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Commits threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of heuristic commits since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when commits exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Rollbacks threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of heuristic rollbacks the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when rollbacks exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Mixed threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of mixed heuristics since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when mixed heuristics exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Hazards threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of heuristic hazards since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when hazards exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

TransResources

Use this Knowledge Script to monitor statistics for transactional resources. This script monitors the transactions that have completed on a WebLogic server since the last sample on a per transactional resource basis. Transactions are rolled back when timeouts or application, system or resource errors occur.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Transactions completed threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions completed since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when transactions completed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions committed threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions committed since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when transactions committed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Transactions rolled back threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of transactions rolled back since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when transactions rolled back exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Description	How to Set It
Heuristic completes threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of heuristic completes since the last sample exceeds this threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when heuristic completes exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

WebAppSessions

Use this Knowledge Script to monitor Web applications. This script monitors the current number of sessions of a Web application and the number of sessions that have been run since the last sample.

Versions of WebLogic Supported

8.1 SP6, 9.0, 9.1, 9.2, and 10.x

Resource Object

WebLogic Server

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default value is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default value is n.
Current sessions threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the current number of sessions of the Web Application exceeds the threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when current sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Peak sessions threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the peak number of concurrent sessions of the Web Application exceeds the threshold, this Knowledge Script raises an event. The default value is –1.
Event severity when peak sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.
Sessions run threshold	Specify a threshold value using an integer greater than or equal to –1. Use –1 to ignore this threshold. If the number of sessions of the Web Application run since the last sample exceeds the threshold, this Knowledge Script raises an event. The default value is 0.
Event severity when sessions run exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 25.

Chapter 72
Web-RT Knowledge Scripts

The Web-RT category provides the following Knowledge Scripts for monitoring Web sites using AppManager ResponseTime for Web.

If you choose to collect data, each Knowledge Script generates the following data streams:

- **Availability.** The availability data point is always one of the following values:
  - 1 or 100 = the test was successful
  - 0 = the test was not successful

  The Availability data point is an indication of whether the response-time test succeeded or failed. If, for example, a connection to the server was established but the test message could not be sent, the Availability data point is 0, which indicates not available or not successful.
- **Response time**. You have two options for collecting response-time data:
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, you can also collect up to 5 response-time breakdown data streams. These data streams are individual data points for the different parts of the Knowledge Script transaction that are timed.

From the Knowledge Script view of the Control Center Console, you can access more information about any Knowledge Script by selecting it and pressing **F1**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
CheckURL	Monitors availability and performance of a single URL, including validating and searching for text, links, and objects. This Knowledge Script is generated from the URL Check Recorder extension.
FTP	Monitors the availability of an FTP site, and verifies that a specified file can be downloaded from the site.
NNTPConnect	Monitors the availability of an NNTP server.
ReceiveInternetMail	Monitors availability and response time to receive an Internet mail message using the POP3 protocol.
Report_Web-RT_Mail	Generates a report of response time and availability for the Web-RT InternetMail Knowledge Scripts.
Report_Web-RT_Steps	Generates a report of response time and availability for the steps in WebTransaction Knowledge Scripts.
Report_Web-RT_URLCheck	Generates a report of percent availability for URL Check Recorder Knowledge Scripts.

Knowledge Script	What It Does
Report_Web-RT_Web	Generates a report of response time and availability for the WebTransaction Knowledge Scripts.
SendAndReceiveInternetMail	Monitors availability and the response time taken to send and receive an Internet mail message using POP3 and SMTP protocols.
SendInternetMail	Monitors availability and the response time taken to send an Internet mail message using the SMTP protocol.
SMTPConnect	Monitors the availability of an SMTP server.
TakeDesktopOwnership	Reassigns control of the desktop on the managed client to AppManager ResponseTime for Web.
URLCheck	Monitors availability and performance of URLs, including validating and searching for text, links, and objects. This Knowledge Script is generated from the URL Check Recorder extension.
WebTransaction	Monitors availability and response time for Web transactions. This Knowledge Script is generated from the Web Recorder extension.

AppManager ResponseTime for Web Version Compatibility

Knowledge Scripts from versions of AppManager ResponseTime for Web earlier than version 6.4 are not supported. New Knowledge Scripts that you create with AppManager ResponseTime for Web 7.x are not backward-compatible and cannot run on older modules.

When you upgrade your version of AppManager ResponseTime for Web, also upgrade all of your managed clients so that they are all at the same level. You must re-record or recreate any Knowledge Scripts you created with versions of Web Recorder older than 2.2 after you install the newer version. You must upgrade all other backlevel Knowledge Scripts. You can do this by opening them in the new recorder, saving them, and checking them back in. Backlevel Knowledge Scripts are not supported unless you upgrade them.

The following table provides a more detailed explanation of version compatibility:

Versions of AppManager ResponseTime for Web and Extensions	Description and Compatibility
ResponseTime for Web 1.2 (shipped with AppManager v5.0.1)	Knowledge Scripts from AppManager for WebServices (WebServices Knowledge Script category) were still supported.
ResponseTime for Web 2.0 (Web-download package)	URL Check Recorder extension replaces WebServices Knowledge Scripts. WebServices and WebTransaction Knowledge Scripts were still supported.
ResponseTime for Web 2.1 (Web-download package)	URL Check Recorder added support for WinHTTP. WebServices and WebTransaction Knowledge Scripts still supported.
ResponseTime for Web 2.2 (Web-download package; shipped with AppManager 6.0)	Major upgrade of Web Recorder. • WebTransaction Knowledge Scripts not backward-compatible. • WebServices and older WebTransaction Knowledge Scripts no longer supported.
ResponseTime for Web 6.2 (Web-download package, and shipped as an additional installation for AppManager 6.0.2)	Major upgrade of Web Recorder. • New WebTransaction Knowledge Scripts not backward-compatible. • Older Knowledge Scripts (v2.2 and later) continue to run. Minor upgrade of URL Check Recorder. • New URLCheck Knowledge Scripts not backward-compatible. • Older Knowledge Scripts (v2.2 and later) continue to run.
ResponseTime for Web 6.3 (Web-download package)	Minor upgrade of Web Recorder. • New WebTransaction Knowledge Scripts not backward-compatible. • Older Knowledge Scripts (v2.2 and later) continue to run. Major upgrade of URL Check Recorder. • New URLCheck Knowledge Scripts not backward-compatible. • Older Knowledge Scripts (v2.2 and later) continue to run.

Versions of AppManager ResponseTime for Web and Extensions	Description and Compatibility
ResponseTime for Web 6.4 (Web-download package)	Upgrade of all Knowledge Scripts. • FTP, InternetMail, NNTPConnect, and SMTPConnect Knowledge Scripts not backward-compatible. • Older Knowledge Scripts (v2.2 and later) continue to run. Major upgrade of Web Recorder. • New WebTransaction Knowledge Scripts not backward-compatible. • Older Knowledge Scripts (v6.2 and later) continue to run. • WebTransaction Knowledge Scripts v2.2 and earlier must be re-recorded. Major upgrade of URL Check Recorder. • New URLCheck Knowledge Scripts not backward-compatible. • Older Knowledge Scripts (v2.2 and later) continue to run.
ResponseTime for Web 7.0 (Shipped with AppManager version 7.0)	Upgrade of all Knowledge Scripts. • FTP, InternetMail, NNTPConnect, and SMTPConnect Knowledge Scripts not backward-compatible in general. • Older Knowledge Scripts (v6.2 and earlier) are **no longer supported**. Minor upgrade of Web Recorder. • New WebTransaction Knowledge Scripts not backward-compatible in general. • Older Knowledge Scripts (v6.2 and earlier) are **no longer supported**. • All backlevel WebTransaction Knowledge Scripts (v6.2 and earlier) must be upgraded or re-recorded. Minor upgrade of URL Check Recorder. • New URLCheck Knowledge Scripts not backward-compatible. • Older Knowledge Scripts (v6.2 and earlier) are **no longer supported**. • All backlevel URLCheck Knowledge Scripts (v6.2 and earlier) must be upgraded or re-recorded.

Versions of AppManager ResponseTime for Web and Extensions	Description and Compatibility
ResponseTime for Web 7.1 (Web-download package)	Upgrade of all Knowledge Scripts. • FTP, InternetMail, NNTPConnect, and SMTPConnect Knowledge Scripts not backward-compatible in general. • Older Knowledge Scripts (v6.2 and earlier) are **no longer supported**. Major upgrade of Web Recorder. • New WebTransaction Knowledge Scripts not backward-compatible in general. • Older Knowledge Scripts (v6.2 and earlier) are **no longer supported**. • All backlevel WebTransaction Knowledge Scripts (v6.2 and earlier) must be upgraded or re-recorded. Major upgrade of URL Check Recorder. • New URLCheck Knowledge Script not backward-compatible. • Older Knowledge Scripts (v6.2 and earlier) are **no longer supported**. • All backlevel URLCheck Knowledge Scripts (v6.2 and earlier) must be upgraded or re-recorded.

CheckURL

Use this Knowledge Script to monitor the availability and performance of a single URL, including measuring connection and download time and validating and searching for text, links, and objects.

The CheckURL Knowledge Script cannot be edited using the URL Check Recorder. This Knowledge Script monitors a single URL, and you can view or modify all available parameter options in the Knowledge Script Values tab, using either the Control Center or Operator Console. To create a custom Knowledge Script that can monitor multiple URLs, use the URL Check Recorder to create a URLCheck Knowledge Script.

Note
You cannot use the Report_Web-RT_URLCheck Knowledge Script to generate reports out of data from the CheckURL Knowledge Script. To report on data from the CheckURL Knowledge Script, use the default reports provided with AppManager. For more information about running default reports, see the Control Center User Guide for AppManager.

Resource Object

CheckURL

Default Schedule

The default interval for these Knowledge Scripts is **Every hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
URL	Specify the URL you want to verify.
Description	Enter the logical description or label of the checked URL.
Logical Target	Enter the identifier to use to enable retrieval of data streams by AppManager Analysis Center v2.0 and higher. By default, either the Label or the Link text for the URL.
General	
Username	Enter the URL authentication username.
Password	Enter the URL authentication password. It is automatically encrypted.
Proxy	
Proxy Server (host:port)	Specify the name of the proxy server computer and port to use, if necessary in your environment, using this format: `host:port`.
User ID	Specify a proxy server username if required. Enter the proxy server username using the format: `username` or `domain\username`.
Password	Specify the proxy server authentication password, if necessary.
Header	Enter a header needed for a function executed on the server. Enter the header using the format: `value:parameter`. AppManager only supports one header.

Post Data	Enter any additional data that the receiving page needs to properly process the request, as in an HTTP Get function. Enter the post data using the format: `value1=parameter&value2=parameter2`. This parameter is optional.
Allow auto-redirects?	Select the **Yes** check box to allow the checked URL to auto-redirect. By default, redirects are allowed. By default, when checking the status of a URL that is redirected, both the original URL and all subsequently redirected URLs are verified, and status is returned for all URLs. This option can be disabled by disabling this parameter.
Uses header with redirections?	Select **Yes** to enable the passing of the header information when this URL is redirected.The default is unselected.
Uses post data with redirections?	Select **Yes** to enable the passing of post data information when this URL is redirected. The default is unselected.
Raise event on redirection?	Select the **Yes** check box to raise an event when the checked URL redirects to one or more subsequent URLs. By default, events are raised.
Number of duplicate redirections before considered looping	Specify the number of times a URL can be redirected to the same location before AppManager raises an event for looping. The default is 1 time. **Notes** • If you set the value to 0, the first duplicate redirection generates a 499 failure. The URL appears once on the detail table. • You can set this value per URL and can modify the value from a running job. • If you keep receiving 499 failures, try increasing this value by 1 and running the job again.
Event severity when URL is redirected	Set the event severity level, from 1 to 40, to indicate the importance of the event raised when the checked URL redirects to one or more subsequent URLs. The default severity level is 20 (yellow event indicator).
Redirect event title	A title for the event raised when the checked URL redirects to one or more subsequent URLs. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. Default is “URL [l] Redirected: [d].”
Details to be included in events	Set to Failure or All. • Failure -- only includes details for failure events or matched event criteria • All -- includes details for all results Default is Failure.
Availability	
Collect data?	Select the **Yes** check box to collect data on the availability of the URL. By default, data is collected.

Details to be saved with data point	Set to Failure, Success, All, or None. • Failure -- Only includes details for failure events or matched event criteria. • Success -- Only includes successful results. • All -- Includes details for all results. • None -- Includes no data details. Default is None.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Web used a 0 ("not available") or 1 ("available") format to indicate availability. You now have the option to use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Data stream legend	A legend for the data stream that measures the availability status of the URL. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. Default is “Availability for URL [d]”. The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.
Raise event on failure	Select the **Yes** check box to raise an event when either the Internet connection or the loading of the base page fails. By default, an event is raised.
Event severity when URL fails	Set the event severity level, from 1 to 40, to indicate the importance of the event raised when a check of the URL fails. Default is 10 (red event indicator).
Failure event title	A title for the event raised when the checked URL returns a status code associated with link failure. For more information, see “Status Code and Status Description” on page 4219. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. Default is “URL [d] Failed”. The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.
Availability = 0 if Validation in error or Search Criteria met	Set to **Yes** to change Availability to **0** if the URL cannot be validated or if a specific text string is not found.
Measure Processing Time	
Collect data?	Select the **Yes** check box to collect data on the processing time taken for this Knowledge Script to run. By default, data is not collected.

Data stream legend	A legend for the data stream that measures the processing time for the URL. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. Default is “Processing Time for URL [d]”. The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.
Threshold -- Maximum processing time	Set the maximum time allowed to perform all operations, including generating data and events, before an event is raised. The default is 180 seconds.
Raise event if threshold exceeded?	Select the **Yes** check box to raise events if the overall time to process the job exceeds the threshold. By default, events are not raised.
Event severity when processing time threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event when the overall processing time threshold is exceeded. The default severity level is 20 (blue event indicator).
Processing Time Event title	A title for the event raised when the processing time for the checked URL exceeds the value you set for the **Threshold -- Maximum overall processing time** parameter. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. Default is “Processing Time Threshold exceeded for URL [d]”. The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.
Measure Connection Time	Select the **Yes** check box to enable connection time measurement. By default, measurement is not enabled.
Collect data?	Select the **Yes** check box to collect data on the amount of time it took to connect to the page represented by the URL and download the first byte of information. By default, data is not collected.
Include DNS Lookup time (if applicable)?	Set to **Yes** to include the time taken to resolve the URL by means of a DNS server in the connection-time measurement. Default is No.
Data stream legend	A legend for the data stream that totals the connection times: the time it takes to connect to the URL and download a single byte of information. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. Default is “Connection Time for URL [d]”. The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.

Threshold -- Maximum connection time	Specify the maximum allowed connection time, in milliseconds. This parameter is the time taken to connect to the checked URL and to download the first byte of information from the associated Web page. If the time taken to connect exceeds this threshold, an event is raised. Default is 1000 milliseconds.
Raise event if threshold exceeded?	Set to **Yes** to raise an event when the amount of time to connect to the specified Web page and download a single byte exceeds the Connection Threshold. Default is Yes.
Event severity when connection time threshold is exceeded	Set the event severity level for the **Measure connection time** threshold from 1 to 40 to indicate the importance of the event raised when the URL download threshold is exceeded. Default severity level is 21 (blue event indicator).
Connection Time Event title	A title for the event raised when the connection time for the URL exceeds the value you set for the **URL connection timeout** parameter. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** column of the URLs table. Default is “URL [d] Connection Time threshold exceeded”. The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.
Connection timeout	Specify a connection timeout in seconds. Default is 10 seconds. Modify this value if connections and downloads are timing out. In most cases, you get an error code of 12002 for timeout conditions.
Measure Download Time	Select the **Yes** check box to enable download time measurement. By default, measurement is not enabled.
Collect data?	Select the **Yes** check box to collect data on the amount of time it takes to download the HTML and associated objects for the checked URL. By default, data is not collected.
Data stream legend	A legend for the data stream that totals the time it takes to download the HTML and associated objects for the checked URL. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. Default is “Download Time for URL [d]”. The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.
Threshold -- Maximum download time	Specify the maximum allowed download time, in milliseconds. This parameter is the time taken to download the HTML and associated objects for the checked URL. If the time taken to download exceeds this threshold, an event is raised. Default is 3000 milliseconds.
Raise event if threshold exceeded?	Set to Yes to raise an event if the download time for the checked URL exceeds the threshold. Default is Yes.

Event severity when download time threshold exceeded	Set the event severity level for the **Measure download time** threshold from 1 to 40 to indicate the importance of the event raised when the URL download threshold is exceeded. Default severity level is 21 (blue event indicator).
Download Time Event title	A title for the event raised when the download time for the URL exceeds the value you set for the **URL download timeout** parameter. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. Default is "URL [d] Download Time threshold exceeded". The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.
Download timeout	Specify a download timeout in seconds. Default is 30 seconds.
Validate All Links	Select the **Yes** check box to enable link validation. By default, validation is not enabled.
Raise event if link validation is in error?	Select **Yes** or **No** to determine whether the Knowledge Script should raise an overall event if any one of the links it checks fails to validate. Link validation failures are defined as links that return HTTP status codes in the 400s or 500s, WinHTTP error codes (12xxxx), or Windows Sockets error codes (11xxxx). The default is Yes. For more information, see "Status Code and Status Description" on page 4219.
Event severity when link validation is in error	Set the event severity level when a link on a page has an HTTP status code or any WinHTTP errors, to indicate the importance of the event. Default is 22 (blue event indicator). For more information, see "Status Code and Status Description" on page 4219.
Validate Links Event title	A title for the event raised when a link fails to validate. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. Default is "URL [d] Validate Link Failure". The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.
Validate All Objects	Use these parameters to determine whether to collect data and raise events on object validation. Select the **Yes** check box to enable object validation. By default, validation is not enabled.

Raise event if object validation is in error?	Select **Yes** or **No** to determine whether the Knowledge Script should raise an overall event any time an object fails to validate. Object validation failures are defined as objects that return HTTP status codes in the 400s or 500s, WinHTTP error codes (12xxxx), or Windows Sockets error codes (11xxxx). The default is Yes. For more information, see “Status Code and Status Description” on page 4219.
Event severity when object validation is in error	Set the event severity level when an object on a page has an HTTP status code or any WinHTTP errors, to indicate the importance of the event. Default is 22 (blue event indicator). For more information, see “Status Code and Status Description” on page 4219.
Validate Objects Event title	A title for the event raised when a link fails to validate. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. Default is “URL [d] Validate Object Failure.” The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.
Search String	Select the **Yes** check box to enable string searching. By default, string searching is not enabled.
String to search	Specify string for search. Specify only 1 string.
Case Sensitive?	If enabled, the search is case-sensitive.
Raise event if string is	Specify whether to raise an overall event when a string meets a selected condition. You can set the Search Strings URL Property for the checked URL, which instructs URL Check Recorder to search for a particular string on the page. The default is “Not Found”.
Event severity when search string criteria are met	Set the event severity level when a string is Found or Not Found, from 1 to 40, to indicate the importance of the event. Default is 25 (blue event indicator).
Search String Event title	A title for the event raised when any specified search string value is met. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. Default is “URL [d] Search String Criteria Met”. The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.
Search Link	Select the **Yes** check box to enable link searching. By default, link searching is not enabled.
Link to search	Specify link for search. Specify only 1 link.
Raise event if link is	Specify whether to generate an event when the specified links are all "Found" or "Not Found". The default is “Not Found”.

Event severity when search link criteria are met	Set the event severity level when a link is Found or Not Found, from 1 to 40, to indicate the importance of the event. Default is 25 (blue event indicator).
Search Link Event title	The title of the event raised when the specified search link value is met. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. The default is “URL [d] Search Link Criteria Met”. The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.
Search Object	Select the **Yes** check box to enable object searching. By default, object searching is not enabled.
Object to search	Specify object for search. Specify only 1 object.
Raise event if object is	Specify whether to raise an event when the specified objects are all "Found" or "Not Found". The default is “Not Found”.
Event severity when search object criteria are met	Set the event severity level when an object is Found or Not Found, from 1 to 40, to indicate the importance of the event. Default is 25 (blue event indicator).
Search Object Event title	The title of the event raised when the specified search object value is met. This field accepts the following substitution variables: • `[l]` -- Substitute the URL address being measured. The URL corresponds to the value you entered in the **URL** parameter. • `[d]` -- Substitute the URL description. The description corresponds to the value you entered in the **Description** parameter. The default is “URL [d] Search ObjectCriteria Met”. The URL variable [l] is not included by default, but you can add the variable anywhere within the legend string.

Status Code and Status Description

For the verified URL, the status code and status description from the Web server are returned. This also applies to any redirected URLs.

URLs that return `1xx`, `2xx` and `3xx` HTTP Status codes are considered successes, while `4xx` or `5xx` HTTP Status codes, WinHTTP error codes (`12xxxx`), or Windows Sockets error codes (`11xxxx`) are considered failures. For more information, see “Status Codes” on page 140.

For more information on HTTP status codes, see:

http://msdn2.microsoft.com/en-us/library/Aa384325.aspx

For more information on WinHTTP error codes, see:

http://msdn2.microsoft.com/en-us/library/Aa383770.aspx

For more information on Windows Sockets error codes, see:

http://msdn2.microsoft.com/en-us/library/ms740668.aspx

FTP

Use this Knowledge Script to check the availability of an FTP site, and verify that a file can be downloaded from the site. In addition, you can use this Knowledge Script to compare the contents of a file downloaded from the FTP site with a file on a local computer.

This Knowledge Script raises an event if any of the following conditions occur:

- The specified FTP site does not respond to the FTP connection request.
- A specified FTP file cannot be downloaded from the site.
- The local file cannot be located.
- The contents of a downloaded FTP file are different from the contents of a specified local file.

If you choose to compare the contents of a downloaded file with the contents of a local file, the Knowledge Script downloads the entire file from the FTP site in both binary and ASCII formats and compares both formats against the local file. An event raised if differences are found between the files after the second comparison. The downloaded file is saved in memory and is never placed on disk. The size of the file to download must be 20 MB or fewer.

The FTP Knowledge Script supports the use of different port numbers, Passive FTP (PASV) for use through a firewall, and connections through a proxy server.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. See the description of the **Event on** parameter in the following table.

If you choose to collect data, a data stream for availability is generated, with one of the following values:

- 1 or 100 = the FTP server responded to the connection request, or
- 0 = the FTP server did not respond.

As discussed previously, this Knowledge Script potentially performs as many as four discrete actions. If any one of the following actions fails, the entire ResponseTime transaction fails, and the Availability data point is 0:

- Connection to the FTP server
- File download
- Opening local file
- Comparing downloaded file to local file

Resource Object

FTP

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect availability data for graphs and reports. If enabled, the Knowledge Script returns: • 1 or 100 = the FTP server responded to the connection request. • 0 = the FTP server did not respond. By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Web used a 0 ("not available") or 1 ("available") format to indicate availability. You now have the option to use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise an event when the FTP server cannot be contacted or the transaction fails. By default, an event is raised.
Event severity when transaction fails	If events are enabled, set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5.
File Download	
Full path and filename to download	Enter the path to the file you want to download from the FTP site, using forward slashes (/) as delimiters. For example: `ftpforms/CAform22.zip` **Notes** You only need to specify the directory in which the file is located and the name of the file. You should not enter a complete, fully qualified URL, for example, `ftp://mysite.com/ftpforms/CAform22.zip`. If you enter a directory path to a local file for the **Full path and filename of local file to compare** parameter, the Knowledge Script can compare the contents of the downloaded file with those of the local file and report any discrepancies. The size of the file to download is limited to 20 MB.

Full path and filename of local file to compare	Enter the path to the local file that you want to use for comparison, using backslashes (\) as delimiters. You can specify a standard path or UNC path. For example:
	`C:\CAforms\CAform22.doc (standard path)`
	`\\CAforms\CAform22.doc (UNC path)`
	This field is case-sensitive.
	Any discrepancies between the files are reported in the Event Details.

Download Time	
Collect data for download time?	Select the **Yes** check box to collect response-time data for graphs and reports. By default, data is collected.
Threshold -- Maximum download time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The event message contains a breakdown of the total response time. The default is 15 seconds.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the response-time threshold is exceeded. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15.

FTP Server	Enter the path to the FTP server that you want to monitor. For example:
	`ftp://ftp.support.com`
	or
	`ftp.support.com`
	Note You can only enter the path to the FTP server itself. You cannot enter a path to a directory on a server, such as `ftp.support.com/files`.
	You can also click **Browse [...]** to select from a list of available FTP servers. The server you select must already be in the TreeView.
	In addition, you can pass a port number following the FTP servername, for example:
	`ftp://ftp.support.com:2100`.)
	If you are setting the **Event on** parameter, the **FTP Server** parameter lets you select the server where the event appears in your console.

Connect using Passive Mode?	Select the **Yes** check box to enable Passive FTP. Passive FTP may be required if the client or server are behind a firewall. By default, Passive FTP is enabled.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** -- The client computer in the response-time tests. This is the default. • **Server** -- The FTP server being tested; see the **FTP Server** parameter. • **Both** -- The event is shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
FTP Logon	
Username	Enter the username to use when connecting to the FTP site that you want to monitor. Type the name exactly as you would when using it to access the FTP site.
Password	Enter the password to use when connecting to the FTP site that you want to monitor. Type the password exactly as you would when using it to access the FTP site. **Note** Password entries are limited to a maximum of 32 characters.
Proxy Settings	
Server name	Specify the name of the proxy server computer and port to use, if necessary in your environment, using this format: `proxyserver:port`
Username	Specify a proxy server username if required. Enter the proxy server username using the format: `username` or `domain\username`.
Password	Specify a proxy server password if required.

NNTPConnect

Use this Knowledge Script to monitor the availability of an NNTP server. When the specified NNTP server does not respond to a connection request to the NNTP port (port 119), an event is raised.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. See the description of the **Event on** parameter in the following table.

If you choose to collect data, a data stream for Availability is generated, with one of the following values:

- 1 or 100 = the NNTP server responded to the connection request, or
- 0 = the NNTP server did not respond.

  The Availability data point is an indication of whether the test succeeded or failed. If a connection to the NNTP server cannot be established, the Availability data point is 0, which indicates not available or not successful.

Resource Object

News (NNTP) server.

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect availability data for graphs and reports. If enabled, the Knowledge Script returns: • 1 or 100 = the NNTP server responded to the connection request. • 0 = the NNTP server did not respond. By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Web used a 0 ("not available") or 1 ("available") format to indicate availability. You now have the option to use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if connection fails?	Select the **Yes** check box to raise events. By default, events are raised.
Event severity when connection fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5 (red event indicator).

NNTP Server	Enter the name of the NNTP server that you want to monitor. For example, `msnews.microsoft.com` You can also click **Browse [...]** to select from a list of available NNTP servers. The server you select must already be in the TreeView. In addition, you can pass a port number following the NNTP servername. For example, `msnews.microsoft.com:563`. If you are setting the **Event on** parameter, the **NNTP Server** parameter lets you select the server where the event appears in your console.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** -- The client computer in the response-time tests. This is the default. • **Server** -- The NNTP server being tested; see the **NNTP Server** parameter. • **Both** -- The event is shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.

ReceiveInternetMail

Use this Knowledge Script to monitor the availability and the response time taken to receive an Internet mail message using POP3 protocol.

You can run this script as "Interactive User." This setting *requires* a user to be physically logged into the computer for the test to run. You might want to do this in environments where a firewall is preventing access to an Active Directory domain controller, or where the test computer is part of a workgroup and not part of a domain. With this feature, the user is not validated, so the test can proceed despite the lack of access to the domain. To run as interactive user, type "`Interactive User`" for the **Run As Username** parameter, and leave the **Password** and **Domain** parameters blank.

Collecting Data

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to 2 response-time breakdown data streams. These are individual data points for the different parts of the Knowledge Script transaction that are timed. For more information, see "Setting Parameter Values" on page 4226.
- **Availability:** Returns one of the following values:
  - 1 or 100 = the transaction was successful
  - 0 = the transaction was not successful

  The Availability data point is an indication of whether the test succeeded or failed. If, for example, a connection to the POP3 mail server was established but the message was never received, the Availability data point is 0, which indicates not available or not successful.

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The Web-RT InternetMail engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is not generated.
- The transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. See the description of the **Event on** parameter in the following table.

Resource Object

Internet Mail

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect availability data for graphs and reports. If enabled, the Knowledge Script returns: • 1 or 100 = the Internet mail server responded to the connection request. • 0 = the Internet mail server did not respond. By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Web used a 0 ("not available") or 1 ("available") format to indicate availability. You now have the option to use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise events. By default, events are raised.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5 (red event indicator).
Response Time	
Collect data for response time?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The event message contains a breakdown of the total response time. The default is 15 seconds.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15 (yellow event indicator). If you disable Response Time events, this value is ignored.
Response Time Breakdown	
Collect data for connecting to POP3 server?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to connect to the POP3 server. By default, separate response-time data streams are not collected.
Collect data for receiving message?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to receive the test Internet Mail message. By default, separate response-time data streams are not collected.
POP3 Server Settings	
Server name	Enter the name of the POP3 server, or click **Browse [...]** to select from a list of available servers. The server you select must already be in the TreeView. If you are setting the **Event on** parameter, the **Target computer** parameter lets you select the server where the event appears in your console.
Server port number	Enter the port number of the POP3 server. Default is 110.
Username	Enter the POP3 username of the client on which the Knowledge Script is to run.
Password	Enter the POP3 password for the associated POP3 user name.
Leave message on server?	Select the **Yes** check box to leave the message on the POP3 server. Clear the box to delete the message from the server. By default, messages are left on the server.

Description	How to Set It
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** -- The client computer in the response-time tests. This is the default. • **Server** -- The mail server being tested; see the **Server name** parameter. • **Both** -- The event is shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Run As	
Username	Enter the user ID associated with a specific user who has the required permissions to run this application. Leave the **Password** and **Domain** parameters blank if you specify "`Interactive User`".
Password	Enter the password associated with this user that is required to log on to the network and run the application.
Domain	Enter the domain name of the domain you are logging onto. Required.
Administrators group on managed client	Enter the name of the Administrators Group on the managed client. Typically, this name is "Administrators", except on some foreign-language operating systems. Default is "Administrators".
Timeouts	
Job timeout	Set the timeout value, from 1 to 900 seconds, to determine the maximum time allowed to process a job before it's aborted. When an Web-RT Knowledge Script job runs, a job timer is started. If the transaction takes longer than the Job timeout, the transaction is stopped and a "Job Timeout" event is raised. The default is 120 seconds.
Queue timeout	Set the timeout value, from 1 to 1200 seconds, to determine how long a job can wait for resources before it's aborted. Multiple simultaneous Web-RT Knowledge Script jobs must wait for a token to run. If no token is available for a job you're trying to run, the job is added to the queue and starts a queue timer. When the Queue Timeout for a job expires, the job does not run, a "Queue Timeout" event is raised, and the job is moved to the end of the queue. The default is 300 seconds.
Connection timeout	Set the connection timeout value to determine how long a job can wait for a connection to the POP3 and SMTP servers before the job is aborted. The default is 30 seconds.

Report_Web-RT_Mail

Use this Knowledge Script to generate a report detailing availability and response time for the following Web-RT Knowledge Scripts:

- ReceiveInternetMail
- SendAndReceiveInternetMail
- SendInternetMail

This report contains twp graphs and tables identifying availability and overall response time for a particular Knowledge Script.

Resource Object

Web-RT

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Knowledge Script for report	Select the Knowledge Script to report on. Click **Browse [...]** to show the Select a Knowledge Script dialog box. Highlight a Web-RT Knowledge Script from the **Knowledge Script Name** list and click **Finish** to select it.
Web-RT client(s)	Select the Web-RT clients. Click **Browse [...]** to show the Select View(s) and a filter dialog box. From the **View(s)** list, select up to 25 views. Your subsequent selections are limited to computers or server groups that are visible in the selected views. Select one of the Filters options: • **View:** Includes all computers in the views you selected. • **Computer:** Select from individual computers in the views you selected. • **Server Group:** Select from server groups in the views you selected. Selecting a server group includes all computers in that group.
Mail Server or “All”	Type the name of the Mail Server, or type “All” to designate all computers as Mail Servers. The default is “All”.
Select time range	In the Select Date/Time Range dialog box, set specific start and end report information dates, good for historical or ad hoc reports, or a sliding range, the default, that sets the time range of data to include in the report. This option is useful for reports running on a regular schedule and is the default.
Select peak weekday(s)	Click **Browse [...]** to see the Select Peak Weekday(s) dialog box. Press **Shift** and click on days to select a contiguous range of days, or **Ctrl+Click** to select non-contiguous days.

Description	How to Set It
Aggregation by	Select the time unit by which to aggregate data. The default is Hour. Works in conjunction with the next field, Aggregation interval, which determines the number of units for one interval of data aggregation.
Aggregation interval	Select the interval units in which to aggregate data. The default is 1. For example, if you aggregate by the Hour and select 1 here, data is aggregated once every hour.
Report settings	
Include parameter card?	Select the Yes check box to include a table in the report that lists parameter settings for the report Knowledge Script. By default, the table is included.
Include Availability detail table?	Specify whether to display the Availability detail table as part of the report. By default, the table is included.
Include Availability chart?	Specify whether to display the Availability chart as part of the report. By default, the chart is included.
Threshold on Availability chart	Enter an integer for the availability, as a percent (%), to use as a threshold on the chart. Default is 0, or no threshold is displayed.
Include ResponseTime detail table?	Specify whether to display the ResponseTime detail table as part of the report. By default, the table is included.
Include ResponseTime chart?	Specify whether to display the ResponseTime chart as part of the report. By default, the chart is included.
Units for ResponseTime report	Select the response time unit, either the default, milliseconds, or seconds.
Threshold on Response Time chart (selected units)	Enter the time in the units specified in the previous parameters to use for the threshold indicator on the chart, or use the default of 0.0, for no threshold indicator is used.
Select chart style	Options in the Chart Settings dialog box set the appearance of the chart. The same parameters are used in both the availability and Response Time charts, if both are produced. Default is Ribbon.
Select output folder	In the Specify report folder/filename dialog box, enter an output filename and fill in the remote folder fields.
Add job ID to output folder name?	Specify whether to add a job ID to the output folder name.
Index-Report Title	In the Report Properties dialog box, configure report title settings.
Add time stamp to title	Specify whether to add a timestamp to the report title.
Event notification	
Generate event on success?	Specify whether an event is raised when a report is generated. By default, events are raised.
Severity level for report success	Set the severity level for a successful report. Default is 35 (magenta event indicator).
Severity level for report with no data	Set the severity level for a report with no data. Default is 25 (blue event indicator).
Severity level for report failure	Set the severity level for a report with no data. Default is 5 (red event indicator).

Report_Web-RT_Steps

Use this Report Knowledge Script to generate a report detailing response time for the transaction steps in WebTransaction Knowledge Scripts created with the Web Recorder extension.

To create this report, enable data collection for individual steps in the selected WebTransaction Knowledge Script. You can also set the *Step default value for "Collect Response Time Data?"* parameter to **Yes** to enable data collection for all steps on a global basis. Click **Settings > Options** and then click the **Knowledge Script** tab in Web Recorder to enable this parameter.

Note
This Knowledge Script only works with WebTransaction Knowledge Scripts that use the default step legends.

Resource Object

Web-RT

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Web Transaction Script	Select the Knowledge Script to report on. Click **Browse [...]** to show the Select a Knowledge Script dialog box. Highlight a Web Transaction Knowledge Script from the Knowledge Script Name list and click **Finish** to select it.
Web-RT client(s)	Select the Web-RT clients. Click **Browse [...]** to show the Select View(s) and a filter dialog box. From the **View(s)** list, select from one to twenty-five views. Your subsequent selections are limited to computers or server groups that are visible in the selected views. Select one of the Filters options: • **View:** Includes all computers in the views you selected. • **Computer:** Select from individual computers in the views you selected. • **Server Group:** Select from server groups in the views you selected. Selecting a server group includes all computers in that group.
Select time range	In the Select Date/Time Range dialog box, set specific start and end report information dates, good for historical or ad hoc reports, or a sliding range, the default, that sets the time range of data to include in the report. This option is useful for reports running on a regular schedule and is the default.
Select peak weekday(s)	Click **Browse [...]** to see the Select Peak Weekday(s) dialog box. Press **Shift** and click on days to select a contiguous range of days, or **Ctrl+Click** to select non-contiguous days.
Aggregation by	Select the time unit by which to aggregate data. Default is Hour. This works in conjunction with the next field, Aggregation interval, which determines the number of units for one interval of data aggregation.

Description	How to Set It
Aggregation interval	Select the interval units in which to aggregate data. Default is 1. For example, if you aggregate by the Hour and select 1 here, data is aggregated once every hour.
Report settings	
Include parameter card?	Select the Yes check box to include a table in the report that lists parameter settings for the report Knowledge Script. By default, the table is included.
Include ResponseTime detail table?	Specify whether to display the ResponseTime detail table as part of the report. By default, the table is included.
Include ResponseTime chart?	Specify whether to display the ResponseTime chart as part of the report. By default, the chart is included.
Units for ResponseTime report	Select the response time unit, either the default, msec, or sec.
Threshold on ResponseTime chart (selected units)	Enter the time in the units specified in the previous parameters to use for the threshold indicator on the chart. The default is 0.0, or no threshold indicator.
Select chart style	Options in the Chart Settings dialog box set the appearance of the chart. The same parameters are used in both the availability and ResponseTime charts, if both are produced. Default is Bar_Stacked.
Select output folder	In the Specify Report Folder/Filename dialog box, enter an output filename and fill in the remote folder fields. Default is Web-RT_Steps_(Script Name)
Add job ID to output folder name?	Specify whether to add a job ID to the output folder name.
Index-Report Title	In the Report Properties dialog box, configure report title settings. Default is Web-RT_Steps:(Script Name)
Add time stamp to title	Specify whether to add a timestamp to the report title. By default, no timestamp is added.
Event notification	
Generate event on success?	Specify whether an event is raised when a report is generated. By default, events are raised.
Severity level for report success	Set the severity level for a successful report. Default is 35 (magenta event indicator).
Severity level for report with no data	Set the severity level for a report with no data. Default is 25 (blue event indicator).
Severity level for report failure	Set the severity level for a report with no data. Default is 5 (red event indicator).

Report_Web-RT_URLCheck

Use this Report Knowledge Script to generate a report of availability as a percentage for the URLCheck Knowledge Script.

This report shows overall availability for all URLs checked by a particular Knowledge Script.

Note
This Knowledge Script only works with URLCheck Knowledge Scripts that use the default legend names. In addition, this Knowledge Script does not work with the CheckURL Knowledge Script. To report on data from the CheckURL Knowledge Script, use the default reports provided with AppManager. For more information about running default reports, see the Control Center User Guide for AppManager.

Set the following parameters as needed:

Description	How to Set It
Data source	
URL Check Script	Select the Knowledge Script to report on. Click **Browse [...]** to show the Select a Knowledge Script dialog box. Highlight a Web Transaction Knowledge Script from the **Knowledge Script Name** list and click **Finish** to select it.
Web Client(s)	Enter a specific client computer, or type `All` to report on all client computers.
Select time range	In the Select Date/Time Range dialog box, set specific start and end report information dates, good for historical or ad hoc reports, or a sliding range, the default, that sets the time range of data to include in the report. This option is useful for reports running on a regular schedule and is the default.
Select peak weekday(s)	Click **Browse [...]** to see the Select Peak Weekday(s) dialog box. Press **Shift** and click on days to select a contiguous range of days, or **Ctrl+Click** to select non-contiguous days.
Aggregation by	Select the time unit by which to aggregate data. Default is Hour. This works in conjunction with the next field, Aggregation interval, which determines the number of units for one interval of data aggregation.
Aggregation interval	Select the interval units in which to aggregate data. Default is 1. For example, if you aggregate by the Hour and select 1 here, data is aggregated once every hour.
Report settings	
Include parameter card?	Select the **Yes** check box to include a table in the report that lists parameter settings for the report Knowledge Script. By default, the table is included.
Include Percent Available detail table?	Specify whether to display the Percent Available detail table as part of the report. By default, the table is included.
Include Percent Available chart?	Specify whether to display the Percent Available chart as part of the report. By default, the chart is included.
Threshold on Percent Available chart (selected units)	Enter an integer for the availability, as a percent (%), to use as a threshold on the chart. Default is 0, or no threshold is displayed.
Select chart style	Options in the Chart Settings dialog box set the appearance of the chart. The same parameters are used in both the availability and ResponseTime charts, if both are produced. Default is Ribbon.
Select output folder	In the Specify report folder/filename dialog box, enter an output filename and fill in the remote folder fields. The default is Web-RT_ Script Name>.
Add job ID to output folder name?	Specify whether to add a job ID to the output folder name.

Index-Report Title	In the Report Properties dialog box, configure report title settings. Default is Web-RT_URLCheck:(Script Name).
Add time stamp to title	Specify whether to add a time stamp to the report title. By default, no timestamp is added.
Event notification	
Generate event on success?	Specify whether an event is raised when a report is generated. By default, events are raised.
Severity level for report success	Set the severity level for a successful report. Default is 35 (magenta event indicator).
Severity level for report with no data	Set the severity level for a report with no data. Default is 25 (blue event indicator).
Severity level for report failure	Set the severity level for a report with no data. Default is 5 (red event indicator).

Report_Web-RT_Web

Use this Report Knowledge Script to generate a report detailing availability and response time for the WebTransaction Knowledge Scripts created with the Web Recorder extension.

This contains two graphs and tables with Availability and overall Response Time for a particular Knowledge Script. For more information, see "Recording a Browsing Session" on page 21.

Note
This Knowledge Script only works with WebTransaction Knowledge Scripts that use the default legend names.

Resource Object

Web-RT

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
WebTransaction Script	Select the Knowledge Script to report on. Click **Browse [...]** to show the Select a Knowledge Script dialog box. Highlight a WebTransaction Knowledge Script from the **Knowledge Script Name** list and click **Finish** to select it.
Web-RT client(s)	Select the Web-RT clients. Click **Browse [...]** to show the Select View(s) and a Filter dialog box. From the **View(s)** list, select from 1 to 25 views. Your subsequent selections are limited to computers or server groups that are visible in the selected views. Select one of the Filters options: • **View:** Includes all computers in the views you selected. • **Computer:** Select from individual computers in the views you selected. • **Server Group:** Select from server groups in the views you selected. Selecting a server group includes all computers in that group.
Select time range	In the Select Date/Time Range dialog box, click **Browse [...]** to set specific start and end report information dates, good for historical or ad hoc reports, or a sliding range, the default, that sets the time range of data to include in the report. This option is useful for reports running on a regular schedule and is the default.
Select peak weekday(s)	Click **Browse [...]** to see the Select Peak Weekday(s) dialog box. Press **Shift** and click on days to select a contiguous range of days, or **Ctrl+Click** to select non-contiguous days.
Aggregation by	Select the time unit by which to aggregate data. The default is Hour. This works in conjunction with the next field, Aggregation interval, which determines the number of units for one interval of data aggregation.

Description	How to Set It
Aggregation interval	Select the interval units in which to aggregate data. The default is 1. For example, if you aggregate by the Hour and select 1 here, data is aggregated once every hour.
Report settings	
Include parameter card?	Select the **Yes** check box to include a table in the report that lists parameter settings for the report Knowledge Script. By default, the table is included.
Include Availability detail table?	Specify whether to display the Availability detail table as part of the report. By default, the table is included.
Include Availability chart?	Specify whether to display the Availability chart as part of the report. By default, the chart is included.
Threshold on Availability chart	Enter an integer for the availability, as a percent (%), to use as a threshold on the chart. Default is 0, or no threshold is displayed.
Include Response Time detail table?	Specify whether to display the Response Time detail table as part of the report. By default, the table is included.
Include Response Time chart?	Specify whether to display the Response Time chart as part of the report. By default, the chart is included.
Units for Response Time report	Select the response time unit, either the default, msec, or sec.
Threshold on Response Time chart (selected units)	Enter the time for the threshold in units specified in the previous parameters, or use the default of 0.0. Zero suppresses the threshold indicator in the chart.
Select chart style	Options in the Chart Settings dialog box set the appearance of the chart. The same parameters are used in both the availability and Response Time charts, if both are produced. Default is Ribbon.
Select output folder	In the Specify report folder/filename dialog box, enter an output filename and fill in the remote folder fields.
Add job ID to output folder name?	Specify whether to add a job ID to the output folder name.
Index-Report Title	In the Report Properties dialog box, configure report title settings.
Add time stamp to title?	Specify whether to add a timestamp to the report title.
Event notification	
Generate event on success?	Specify whether an event is raised when a report is generated. By default, events are raised.
Severity level for report success	Set the severity level for a successful report. Default is 35 (magenta event indicator).
Severity level for report with no data	Set the severity level for a report with no data. Default is 25 (blue event indicator).
Severity level for report failure	Set the severity level for a report with no data. Default is 5 (red event indicator).

SendAndReceiveInternetMail

Use this Knowledge Script to monitor the response time taken to send and receive an Internet mail message using the POP3 and SMTP protocols.

You can run this script as "Interactive User." This setting *requires* a user to be physically logged into the computer for the test to run. You might want to do this in environments where a firewall is preventing access to an Active Directory domain controller, or where the test computer is part of a workgroup and not part of a domain. With this feature, the user is not validated, so the test can proceed despite the lack of access to the domain. To run as interactive user, type "`Interactive User`" for the **Run As Username** parameter, and leave the **Password** and **Domain** parameters blank.

Collecting Data

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to 5 response-time breakdown data streams. These data streams are individual data points for the different parts of the Knowledge Script transaction that are timed. For more information, see "Setting Parameter Values" on page 4237.
- **Availability:** Returns one of the following values:
  - 1 or 100 = the transaction was successful
  - 0 = the transaction was not successful

  The Availability data point is an indication of whether the test succeeded or failed. If, for example, a connection to the POP3 mail server was established but the message was never sent, the Availability data point is 0, which indicates not available or not successful.

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The Web-RT InternetMail engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is not generated.
- The transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. See the description of the **Event on** parameter in the following table.

Resource Object

Internet Mail

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect availability data for graphs and reports. If enabled, the Knowledge Script returns: • 1 or 100 = the server responded to the connection request. • 0 = the server did not respond. By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Web used a 0 ("not available") or 1 ("available") format to indicate availability. You now have the option to use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise events. By default, events are raised.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5 (red event indicator).
Response Time	
Collect data for response time?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The event message contains a breakdown of the total response time. The default is 15 seconds.
Raise event when threshold is exceeded?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are raised.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15 (yellow event indicator). If you disable Response Time events, this value is ignored.
Response Time Breakdown	
Collect data for connecting to SMTP server?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to connect to the SMTP server. By default, separate response-time data streams are not collected.
Collect data for sending message?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to send the test message. By default, separate response-time data streams are not collected.
Collect data for connecting to POP3 server?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to connect to the POP3 server. By default, separate response-time data streams are not collected.
Collect data for scanning incoming mail for message?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to check the mailbox for the test message. By default, separate response-time data streams are not collected.
Collect data for receiving message?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to receive the test message. By default, separate response-time data streams are not collected.
SMTP Server Settings	

Description	How to Set It
Server name	Enter the name of the SMTP server, or click **Browse [...]** to select from a list of available servers. The server you select must already be in the TreeView. If you are setting the **Event on** parameter, the **Server name** parameter lets you select the server where the event appears in your console.
Server port number	Enter the port number of the SMTP server. Default is 25.
POP3 Server Settings	
Server name	Enter the name of the POP3 server, or click **Browse [...]** to select from a list of available servers. The server you select must already be in the TreeView. If you are setting the **Event on** parameter, the **Server name** parameter lets you select the server where the event appears in your console.
Server port number	Enter the port number of the POP3 server. Default is 110.
Username	Enter the POP3 username of the client where you are running this Knowledge Script.
Password	Enter the POP3 password for the associated POP3 user name.
Email address	Enter the email address of the client where you are running this Knowledge Script job.
Message size	Enter the number of bytes to include as text in the message body. Default is 1000.
Leave message on server?	Select the **Yes** check box to leave the message on the POP3 server. Clear the box to delete the message from the server. By default, messages are left on server.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** -- The client computer in the response-time tests. This is the default. • **Server** -- The mail server being tested; see the **Server name** parameter for the POP3 or SMTP server. • **Both --** The event is shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Run As	
Username	Enter the user ID associated with a specific user who has the required permissions to run this application. Leave the **Password** and **Domain** parameters blank if you specify "`Interactive User`".
Password	Enter the password associated with this user that is required to log on to the network and run the application.
Domain	Enter the domain name of the domain you are logging onto.
Administrators group on managed client	Enter the name of the Administrators Group on the managed object. Typically, this name is "Administrators", except on some foreign-language operating systems. The default is "`Administrators`".
Timeouts	

Description	How to Set It
Job timeout	Set the timeout value, from 1 to 900 seconds, to determine the maximum time allowed to process a job before it's aborted. When an Web-RT Knowledge Script job runs, a job timer is started. If the transaction takes longer than the Job timeout, the transaction is stopped and a “Job Timeout" event is raised. The default is 120 seconds.
Queue timeout	Set the timeout value, from 1 to 1200 seconds, to determine how long a job can wait for resources before it's aborted. Multiple simultaneous Web-RT Knowledge Script jobs must wait for a token to run. If no token is available for a job you're trying to run, the job is added to the queue and starts a queue timer. When the Queue Timeout for a job expires, the job does not run, a "Queue Timeout" event is raised, and the job is moved to the end of the queue. The default is 300 seconds.
Connection timeout	Set the connection timeout value to determine how long a job can wait for a connection to the POP3 and SMTP servers before the job is aborted. The default is 30 seconds.

SendInternetMail

Use this Knowledge Script to monitor the response time taken to send an Internet mail message using the SMTP protocol.

You can run this script as "Interactive User." This setting *requires* a user to be physically logged into the computer for the test to run. You might want to do this in environments where a firewall is preventing access to an Active Directory domain controller, or where the test computer is part of a workgroup and not part of a domain. With this feature, the user is not validated, so the test can proceed despite the lack of access to the domain. To run as interactive user, type "`Interactive User`" for the **Run As Username** parameter, and leave the **Password** and **Domain** parameters blank.

Collecting Data

If you choose to collect data, this Knowledge Script generates the following data streams:

- **Response time**
  - **Overall response time**. The information returned by this data stream is also saved with the data point, and can be viewed by double-clicking the data point in the Graph Pane or Chart Console.
  - **Response-time Breakdown**. If enabled as separate parameters, up to 2 response-time breakdown data streams. These data streams are individual data points for the different parts of the Knowledge Script transaction that are timed. For more information, see "Setting Parameter Values" on page 4241.
- **Availability:** Returns one of the following values:
  - 1 or 100 = the transaction was successful
  - 0 = the transaction was not successful

  The Availability data point is an indication of whether the test succeeded or failed. If, for example, a connection to the POP3 mail server was established but the message was never sent, the Availability data point is 0, which indicates not available or not successful.

An event is raised whenever one of the following occurs:

- A threshold that you have specified as an event parameter is exceeded.
- The Web-RT InternetMail engine cannot be initialized. An initialization error is generated, but an Availability or Response Time data stream is not generated.
- The transaction does not complete successfully. A transaction error is generated. Only an Availability data stream is generated, with a value of 0.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. See the description of the **Event on** parameter in the following table.

Resource Object

Internet Mail

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect availability data for graphs and reports. If enabled, the Knowledge Script returns: • 1 or 100 = the server responded to the connection request. • 0 = the server did not respond. By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Web used a 0 ("not available") or 1 ("available") format to indicate availability. You now have the option to use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if transaction fails?	Select the **Yes** check box to raise events. By default, events are raised.
Event severity when transaction fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5 (red event indicator).
Response Time	
Collect data for response time?	Select the **Yes** check box to collect data for graphs and reports. By default, data is collected.
Threshold -- Maximum response time (seconds)	Specify the maximum response time in seconds. When response time exceeds this value, an event is raised. The event message contains a breakdown of the total response time. The default is 15 seconds.
Raise event when threshold is exceeded?	Select the **Yes** check box to raise an event when the threshold is exceeded. By default, events are raised.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 15 (yellow event indicator). If you disable Response Time events, this value is ignored.
Response Time Breakdown	
Collect data for connecting to SMTP server?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to connect to the SMTP server. By default, separate response-time data streams are not collected.
Collect data for sending message?	Select the **Yes** check box to collect a separate response-time data stream for the time taken to send the test message. By default, separate response-time data streams are not collected.
SMTP Server Settings	
Server name	Enter the name of the SMTP server, or click **Browse [...]** to select from a list of available servers. The server you select must already be in the TreeView. If you are setting the **Event on** parameter, the **Server name** parameter lets you select the server where the event appears in your console.
Server port number	Enter the port number of the SMTP server. Default is 25.
Email address	Enter the email address of the client where the Knowledge Script job runs.
Message size	Enter the number of bytes to include as text in the message body. Default is 1000.

Description	How to Set It
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** -- The client computer in the response-time tests. This is the default. • **Server** -- The mail server being tested; see the **Server name** parameter. • **Both** -- The event is shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Run As	
Username	Enter the user ID associated with a specific user who has the required permissions to run this application. Leave the **Password** and **Domain** parameters blank if you specify "`Interactive User`".
Password	Enter the password associated with this user that is required to log on to the network and run the application.
Domain	Enter the domain name of the domain you are logging onto.
Administrators group on managed client	Enter the name of the Administrators Group on the managed object. Typically, this name is "Administrators", except on some foreign-language operating systems. The default is "`Administrators`".
Timeouts	
Job timeout	Set the timeout value, from 1 to 900 seconds, to determine the maximum time allowed to process a job before it's aborted. When an Web-RT Knowledge Script job runs, a job timer is started. If the transaction takes longer than the Job timeout, the transaction is stopped and a "Job Timeout" event is raised. The default is 120 seconds.
Queue timeout	Set the timeout value, from 1 to 1200 seconds, to determine how long a job can wait for resources before it's aborted. Multiple simultaneous Web-RT Knowledge Script jobs must wait for a token to run. If no token is available for a job you're trying to run, the job is added to the queue and starts a queue timer. When the Queue Timeout for a job expires, the job does not run, a "Queue Timeout" event is raised, and the job is moved to the end of the queue. The default is 300 seconds.
Connection timeout	Set the connection timeout value to determine how long a job can wait for a connection to the POP3 and SMTP servers before the job is aborted. The default is 30 seconds.

SMTPConnect

Use this Knowledge Script to monitor the availability of an SMTP server. When the specified SMTP server does not respond to a connection to the SMTP port (port 25), an event is raised.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. See the description of the **Event on** parameter in the following table.

If you choose to collect data, a data stream for Availability is generated, with one of the following values:

- 1 or 100 = the SMTP server responded to the connection request, or
- 0 = the SMTP server did not respond.

  The Availability data point is an indication of whether the test succeeded or failed. If a connection to the SMTP server cannot be established, the Availability data point is 0, which indicates not available or not successful.

Resource Object

SMTP

Default Schedule

The default interval for this Knowledge Script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Availability	
Collect data for availability?	Select the **Yes** check box to collect availability data for graphs and reports. If enabled, the Knowledge Script returns: • 1 or 100 = the SMTP server responded to the connection request. • 0 = the SMTP server did not respond. By default, data is collected.
Data stream format	Select the data stream format for the Availability data stream. Previous versions of AppManager ResponseTime for Web used a 0 ("not available") or 1 ("available") format to indicate availability. You now have the option to use a 0 ("not available") or 100 ("available") format. The default value is 0-100.
Raise event if connection fails?	Select the **Yes** check box to raise events. By default, events are raised.
Event severity when connection fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. Default is 5 (red event indicator).

SMTP Server	Enter the name of the SMTP server that you want to test. For example, `gazelle.netiq.com`. You can also click **Browse [...]** to select from a list of available servers. The server you select must already be in the TreeView. If you are setting the **Event on** parameter, the **SMTP Server** parameter lets you select the server where the event appears in your console. You can also pass a port number following the SMTP servername. For example, you can enter `gazelle.netiq.com:2500`.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** -- The client computer in the response-time tests. This is the default. • **Server** -- The mail server being tested; see the **SMTP Server** parameter. • **Both** -- The event is shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.

TakeDesktopOwnership

Use this Knowledge Script to reassign control of the desktop on the managed client computer when another module is controlling it.

Note
You only need to run this Knowledge Script if you are also using AppManager ResponseTime for Windows and you want to run Web-RT_WebTransaction Knowledge Scripts and Win-RT Knowledge Scripts on the same managed client.

Both Win-RT and Web-RT_WebTransaction Knowledge Scripts must have control of the desktop in order to run or play back. However, only one software application can control the desktop at any point. When a WebTransaction Knowledge Script runs, it checks for the value of the "`Desktop`" registry key on the managed client. If that value assigns control of the desktop to another software application, the Knowledge Script fails and displays a Playback error.

Use this Knowledge Script to overwrite any existing value for the "`Desktop`" registry key, located under `HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\Response Time`, and force control of the desktop to be granted to AppManager ResponseTime for Web.

Resource Object

Web-RT

Default Schedule

The default interval for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when take desktop ownership fails?	Specify a severity level for the event raised when an error prevents the Knowledge Script from setting the registry value indicating that AppManager ResponseTime for Web has ownership of the desktop. Default is 5 (red event indicator).
Raise event if take desktop ownership successful?	Check the box to raise an event when the Knowledge Script updates the registry value indicating that AppManager ResponseTime for Web has ownership of the desktop. By default, events are not raised.
Event severity when take desktop ownership successful?	Specify a severity level for the event raised when the Knowledge Script updates the registry value indicating that AppManager ResponseTime for Web has ownership of the desktop. Default is 35 (magenta event indicator).

URLCheck

Use this Knowledge Script to monitor the availability and performance of URLs, including validating and searching for text, links, and objects. This Knowledge Script is generated by the **URL Check Recorder** extension.

The URL Properties configured in URL Check Recorder are distinct settings and cannot be edited in the Knowledge Script itself. The Knowledge Script parameters, which for the most part are determined by URL Check Recorder settings when the Knowledge Script was created, let you further configure or change Knowledge Script execution and results collection. You can make an additional set of customizations by editing the Knowledge Script Options, which let you determine the titles of events and data streams. To change these options or the URL Properties, you can check out the Knowledge Script, reopen it in URL Check Recorder, edit it, save it, and check it back in.

Knowledge Scripts created using the URL Check Recorder are different from the provided CheckURL Knowledge Script. The CheckURL Knowledge Script monitors a single URL and can only be modified using the Control Center or Operator Console. For more information, see "CheckURL" on page 4212.

Note
Context-sensitive Help is not available for URLCheck Knowledge Scripts. To access Help for URLCheck Knowledge Scripts, launch the Help for AppManager. In the Table of Contents pane of the Help window, click Knowledge Script Reference, then Web-RT Knowledge Scripts. Scroll through the table shown in the right pane and click URLCheck to view Help for these Knowledge Scripts.

Resource Object

URL Check

Default Schedule

The default interval for these Knowledge Scripts is **Every hour**.

Setting Parameter Values

Set the following parameters as needed. This table includes all available parameters. Depending on how you configure URLCheck options for a particular Knowledge Script, some parameters may not be available.

Description	How to Set It
General	
Allow auto-redirects?	Select the **Yes** check box to allow auto-redirects of URLs. By default, redirects are allowed.
Details to be included in events	Set to `Failure` to collect details only on failure events, or `All` to collect for all results. Default is Failure.
Logical Target	Enter the identifier to use to enable retrieval of data streams by AppManager Analysis Center v2.0 and higher. By default, either the Label or the Link text for the first URL.
Overall Availability	
Collect data (%)?	Select the **Yes** check box to collect data on the availability of the URLs as a percentage (%). By default, data is collected.

Threshold -- Minimum overall URL availability (%)	Specify a threshold for the percentage of URLs that are available. Default is 100%.
Raise event when overall URL availability falls below threshold?	Select the **Yes** check box to raise an event when the number of available URLs falls below the threshold. By default, events are raised.
Details to be saved with Overall URL Availability data point	Set to Failure, Success, All, or None. • Failure -- Only includes details for failure events or matched event criteria. • Success -- Only includes successful results. • All -- Includes details for all results. • None -- Includes no data details. Default is None.
Individual Availability	
Individual URL Availability data stream format	Select the data stream format for the individual URL Availability data stream. Previous versions of AppManager ResponseTime for Web used a 0 (“not available”) or 1 (“available”) format to indicate availability. You now have the option to use a 0 (“not available”) or **100** (“available”) format. The default value is 0-100.
Overall Processing Time	
Collect data?	Select the **Yes** check box to collect data on the overall processing time taken for this Knowledge Script to run. By default, data is not collected.
Threshold -- Maximum overall processing time	Set the maximum time allowed to perform all operations, including generating data and events, before an event is raised. The default is 180 seconds.
Raise event if threshold exceeded?	Select the **Yes** check box to raise events if the overall time to process the job exceeds the threshold. By default, events are not raised.
Timeouts	Use these parameters to set timeouts.
URL connection timeout	Specify a connection timeout in seconds. Default is 10 seconds.
URL download timeout	Specify a download timeout in seconds. Default is 30 seconds.
Event Severity	
Event severity when URL fails	Set the event severity level, from 1 to 40, to indicate the importance of the event raised when a check of an individual URL fails. Default is 10 (red event indicator).
Event severity when overall URL availability falls below threshold	Set the event severity level from 1 to 40 to indicate the importance of the event raised when the **Threshold -- Minimum overall URL availability (%)** is not met. Default is 15 (yellow event indicator).
Event severity when processing time threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event when the overall processing time threshold is exceeded. The default severity level is 20 (blue event indicator).
Event severity when URL is redirected	Set the event severity level, from 1 to 40, to indicate the importance of the event raised when a checked URL redirects to one or more subsequent URLs. The default severity level is 20 (yellow event indicator).
Event severity when connection time threshold is exceeded	Set the event severity level for the **Measure connection time** threshold from 1 to 40 to indicate the importance of the event raised when the URL download threshold is exceeded. Default severity level is 21 (blue event indicator).

Event severity when download time threshold is exceeded	Set the event severity level for the **Measure download time** threshold from 1 to 40 to indicate the importance of the event raised when the URL download threshold is exceeded. Default severity level is 21 (blue event indicator).
Event severity when link validation is in error	Set the event severity level when a link on a page has an HTTP status code or any WinHTTP errors, to indicate the importance of the event. Default is 22 (blue event indicator). For more information, see "Status Code and Status Description" on page 4248.
Event severity when object validation is in error	Set the event severity level when an object on a page has an HTTP status code or any WinHTTP errors, to indicate the importance of the event. Default is 22 (blue event indicator). For more information, see "Status Code and Status Description" on page 4248.
Event severity when search string criteria are met	Set the event severity level when a string is Found or Not Found, from 1 to 40, to indicate the importance of the event. Default is 25 (blue event indicator).
Event severity when search link criteria are met	Set the event severity level when a link is Found or Not Found, from 1 to 40, to indicate the importance of the event. Default is 25 (blue event indicator).
Event severity when search object criteria are met	Set the event severity level when an object is Found or Not Found, from 1 to 40, to indicate the importance of the event. Default is 25 (blue event indicator).
Collect data for Total of Connection Times?	Select the **Yes** check box to collect data on the time it took, in seconds, to connect to each Web page and download the first byte of information from each. By default, data is not collected.
Collect data for Total of Download Times?	Select the **Yes** check box to collect data on the time it took, in seconds, to fully download all Web pages, including the HTML and all associated components. By default, data is not collected.

Status Code and Status Description

For each URL that is verified, the status code and status description from the Web server are returned. This also applies to redirected URLs.

URLs that return `1xx`, `2xx` and `3xx` HTTP Status codes are considered successes, while `4xx` or `5xx` HTTP Status codes, WinHTTP error codes (`12xxxx`), or Windows Sockets error codes (`11xxxx`) are considered failures. For more information, see "Status Codes" on page 140.

For more information on HTTP status codes, see:

http://msdn2.microsoft.com/en-us/library/Aa384325.aspx

For more information on WinHTTP error codes, see:

http://msdn2.microsoft.com/en-us/library/Aa383770.aspx

For more information on Windows Sockets error codes, see:

http://msdn2.microsoft.com/en-us/library/ms740668.aspx

Redirects

By default, when checking the status of a URL that is redirected, both the original URL and all subsequently redirected URLs are verified, and status is returned for all URLs. This option can be disabled by disabling the **Allow Auto-Redirects?** parameter.

Timeouts

The URL connection timeout and URL download timeouts can be modified if connections and downloads are timing out. In most cases, you get an error code of 12002 for timeout conditions. For more information, see "Problems with URL Check Recorder" on page 199.

WebTransaction

The Web Recorder extension lets you record a typical set of user transactions on a Web site and save this information as an AppManager Knowledge Script. When you check in the new Knowledge Script, it is added to the Web-RT category by default.

You can then run the Knowledge Script on any computer that has the Web-RT module installed. The generated Knowledge Script allows you to monitor the availability and response time required to complete the entire transaction, as well as the individual steps within the transaction.

You can select where some of the possible events are displayed in the Operator Console TreeView or Control Center Console Server view. This event proxying feature is useful in Control Center Service Map views. It is not supported for jobs that are started in the Operator Web Console. See the description of the **Event on** parameter in the following table.

Each WebTransaction Knowledge Script contains all information you entered while performing and recording the transaction. Any information that is encrypted during the recorded browsing session is also encrypted in the resulting Knowledge Script.

Note
When you generate WebTransaction Knowledge Scripts with Web Recorder, you rename them in order to save the contents of each transaction. However, this means that the context-sensitive Help no longer works from the renamed Knowledge Scripts. To access Help for WebTransaction Knowledge Scripts, launch the Help for AppManager. In the left pane of the Help window, click Knowledge Script Reference in the Table of Contents, then click Web-RT Knowledge Scripts to see the table of Knowledge Script types.

Resource Object

Web Transaction

Default Schedule

The default interval for this Knowledge Script type is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General	
Run in silent mode?	Select the **Yes** check box to instruct the Knowledge Script to play back without displaying anything on the computer screen. **Note** Silent mode is not available if the Knowledge Script contains any steps that have the `MouseMove` option enabled. By default, silent mode is enabled.
Execution speed	Set to `Slow`, `Medium`, or `Fast` to determine how fast the Knowledge Script plays back on the managed client. This parameter is controlled by means of the Playback Speed function in Web Recorder. By default, the execution speed is set to Medium. Refer to the Web Recorder online Help for the values.

Description	How to Set It
Logical Target	Enter an identifier to use to enable retrieval of all data streams in AppManager Analysis Center v2.0 and higher. By default, this field is set with information from the first Navigate step. It may be, for example, the URL of the page accessed.
Target Computer	Enter an identifier to use to enable retrieval of all data streams in AppManager Analysis Center v2.0 and higher. Select the name of the target Web server for the transaction from the list of monitored Web servers. If you are setting the **Event on** parameter, the **Target Computer** parameter lets you select the server where the event appears in your console. This field may be left blank, which is the default setting.
Log Session Transcript?	Select the **Yes** check box to create a log file containing the session transcript of the Knowledge Script Playback. If enabled, saves the log file in the `..\NetIQ\AppManager\temp\netiq_debug\[computername]` directory. The log filename is `Web-RT[JobNumber]Transcript.log`. By default, no log is created. **Note** This option should only be enabled to aid in the debugging of problems.
Event on	Select the TreeView location where events should be displayed. Select either: • **Agent** -- The client computer in the response-time tests. This is the default. • **Server** -- The Web server being tested; see the **Target Computer** parameter. • **Both** -- The event is shown in two locations in the TreeView. **Notes** This setting does not apply to events related to the Knowledge Script itself, such as Knowledge Script failure or initialization problems. Such events are always displayed on the computer where the job ran. You must select `Agent` when starting jobs in the Operator Web Console. If you select `Server`, no events are generated. If you select `Both`, an event is only shown on the agent.
Capture browser snapshot when object not found?	Select the **Yes** check box to instruct Web Recorder to take a screen capture of the browser window if the step fails because an object is not found. Enable this parameter to take a screen capture in JPEG (`.jpg`) format. The image file is saved to `..\NetIQ\temp\netiq_debug\[ComputerName]`. The filename begins with “WebTransaction” and the job ID number, and it includes the time and date. **Tip** To ensure that the screen capture shows the entire page, re-record the transaction. While recording, click **Maximize** in the browser window. When you return to the Web Recorder window, a Resize Browser step is available. Set the coordinates as needed to make the browser window as large as possible. See the following parameter for another snapshot option.
Capture HTML snapshot when object not found?	Select the **Yes** check box to instruct Web Recorder to take a snapshot of the browser window if the step fails because an object is not found. Enable this parameter to take a screen capture in HTML (`.htm`) format. The HTML file is saved to `..\NetIQ\temp\netiq_debug\[ComputerName]`. The filename begins with “WebTransaction” and the job ID number, and it includes the time and date. See the previous parameter for another snapshot option.

Description	How to Set It
Capture browser snapshot on Navigate Errors?	Select the **Yes** check box to instruct Web Recorder to take a screen capture of the browser window if the step fails because of a Navigate Error. Enable this parameter to take a screen capture in JPEG (`.jpg`) format. The image file is saved to `..\NetIQ\temp\netiq_debug\[ComputerName]`. The filename begins with "WebTransaction" and the job ID number, and it includes the time and date. **Tip** To ensure that the screen capture shows the entire page, re-record the transaction. While recording, click **Maximize** in the browser window. When you return to the Web Recorder window, a Resize Browser step is available. Set the coordinates as needed to make the browser window as large as possible. See the following parameter for another snapshot option.
Capture HTML snapshot on Navigate Errors?	Select the **Yes** check box to instruct Web Recorder to take a snapshot of the browser window if the step fails because of a Navigate Error. Enable this parameter to take a screen capture in HTML (`.htm`) format. The HTML file is saved to `..\NetIQ\temp\netiq_debug\[ComputerName]`. The filename begins with "WebTransaction" and the job ID number, and it includes the time and date. See the previous parameter for another snapshot option.
Capture extra snapshot?	Select the **Yes** check box if previous snapshots were taken too early and provided irrelevant information. Enabling this option might allow the Web Recorder to take additional snapshots of the browser window. Enabling this option increases the chance that you may capture a snapshot with better information about the problem. Web Recorder might take many extra snapshots, or none at all depending on the behavior of the Web page itself.
Overall Availability	
Collect data?	Select the **Yes** check box to collect data on the overall availability of the Web sites tested by this Knowledge Script. By default, data is collected.
Overall Response Time	
Collect data?	Select the **Yes** check box to collect data on the overall availability of the Web sites tested by this Knowledge Script. By default, data is collected. **Note** You can specify *not* to include data collected on individual steps in overall response time.
Threshold -- Maximum overall response time	Set the maximum response time that can be calculated for all steps in the transaction as a whole before an event is raised. The default is 120 seconds.
Raise event if threshold exceeded?	Select the **Yes** check box to raise events if the overall response time threshold is exceeded. By default, events are not raised.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 15 (yellow event indicator).
Overall Processing Time	
Collect data?	Select the **Yes** check box to collect data on the overall processing time taken for this Knowledge Script to run. By default, data is not collected.
Threshold -- Maximum overall processing time	Set the maximum time that can be taken to run the entire recorded transaction before an event is raised. The default is 180 seconds.
Raise event if threshold exceeded?	Select the **Yes** check box to raise events if the overall processing time threshold is exceeded. By default, events are not raised.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event when the overall processing time threshold is exceeded. The default severity level is 20 (yellow event indicator).

Description	How to Set It
Timers	Use these parameters to determine timeouts and set boundaries for discrete transaction steps. **Note** Time added to a Knowledge Script from one of these timers is not included in response-time measurements, which is returned as the Total Response Time. It is only included in the Total Processing Time shown in the results.
Queue timeout	Set the timeout value, from 1 to 60 minutes, to determine how long a job can wait for resources before it is aborted. Multiple simultaneous WebTransaction Knowledge Script jobs must wait for a token to run because they all depend on Internet Explorer. If no token is available for a job you are trying to run, the transaction is added to the queue and starts a queue timer. When the queue timeout for a job expires, the transaction does not run, a "Queue Timeout" event is raised, and the transaction is moved to the end of the queue. The default is 5 minutes.
Job timeout	Set the timeout value, from 1 60 minutes, to determine the maximum time allowed to process a job before it is aborted. When a WebTransaction Knowledge Script job runs, a job timer is started. If the transaction takes longer than the job timeout, the transaction is stopped and a "Job Timeout" event is raised. This avoids allowing any job to use Internet Explorer resources for too long. The default is 5 minutes. **Note** The Total Processing Time shown in the results after Playback is a guideline for determining an appropriate job timeout value: the job timeout value should be slightly greater than the maximum Total Processing Time.
Consider document complete *N* seconds after page change	Set the value, from 1 to 30 seconds, to determine how long Web Recorder should wait after a Web page transition event to consider the page download complete. This timer lets Web Recorder complete a transaction step even if it never receives the `Document Complete` signal from Internet Explorer to indicate that the page has been fully loaded. The default is 20 seconds.
Consider document complete *N* seconds after Download Complete	Set the value, from 5 to 300 seconds, to determine how long Web Recorder should wait after receiving a `Download Complete` signal from Internet Explorer to consider the page to be completely loaded. This timer lets Web Recorder complete a transaction step even if it never receives the proper signal from Internet Explorer to indicate that the new page has been fully loaded. The default is 10 seconds.
Delay after document complete	Set the value, from 0 to 10 seconds, to determine whether and how long Web Recorder should pause before moving on to a new step. Internet Explorer can sometimes send several "final" `Document Complete` signals. Web Recorder may therefore consider the step to be complete at the first `Document Complete` signal, before all objects are actually rendered. This option means that Web Recorder waits for up to 10 seconds after it has determined that the step is complete before it moves on to the next step, giving all objects a further opportunity to be retrieved. The default is 1 second.
Global Step Options	
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event when the response time for any individual step exceeds its threshold. The default severity level is 16 (yellow event indicator).

Description	How to Set It
Event severity when step fails	Set the event severity level, from 1 to 40, to indicate the importance of the event when any individual step fails. The default severity level is 10 (red event indicator).
Event severity on Navigate Error	Set the event severity level, from 1 to 40, to indicate the importance of the event when any individual step fails because of a Navigate Error. The default severity level is 18 (yellow event indicator).
Step [n] [x] [d]	Use the parameters in the individual step folders to set options for data collection, to define threshold values, and to enable events. Each step is identified by its step index number (variable n), its step type (variable x), and a step description (variable d). For more information, see "Step-Identifying Variables" on page 77.
Collect data for availability?	Select the **Yes** check box to collect data on the availability of the Web page accessed by this step. By default, data is not collected, but this value depends on what you have set in the **Knowledge Script** tab of the Web Recorder Options.
Collect data for response time?	Select the **Yes** check box to collect data on the response time taken to load the Web page accessed by this step. By default, data is not collected, but this value depends on what you have set in the **Knowledge Script** tab of the Web Recorder Options.
Included in Overall Response Time?	Select the **Yes** check box to include collected data in the Overall Response Time. By default, data is included. **Note** Ensure you include the collected data from at least one step, or your overall response time is zero.
Threshold -- Maximum response time	Set the maximum time that can be taken to complete this transaction step before an event is raised. The default is 30 seconds. This value depends on what you have set in the **Knowledge Script** tab of the Web Recorder Options.
Raise event if threshold is exceeded?	Select the **Yes** check box to raise events if the response time threshold is exceeded. By default, events are enabled. The event severity that you set in the Global Step Options folder applies to this event.

Chapter 73
WebSphereAppSrvUNIX Knowledge Scripts

The WebSphereAppSrvUNIX category provides Knowledge Scripts for monitoring IBM WebSphere Application Servers.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Administrative Knowledge Scripts

The following Knowledge Scripts perform administrative tasks associated with IBM WebSphere Application Server:

Knowledge Script	What It Does
NetIQAgent	Starts or stops the Java server that the managed object uses to communicate with IBM WebSphere Application Server.
SetRMFilters	Sets filters for logging request metrics traces.
SetServerLogPath	Sets the path of the server's primary JVM log file.
StartServer	Starts an application server instance.
StopServer	Stops an application server instance.

Dynamic Cache Knowledge Scripts

The following Knowledge Scripts are focused on the dynamic cache:

Knowledge Script	What It Does
DynamicCacheEviction	Returns the number of local and remote requests made.
DynamicCacheHits	Returns the number of cache hits in memory and on disk, and the number of cache misses.

Enterprise Java Bean Knowledge Scripts

The following Knowledge Scripts are focused on Enterprise Java Beans (EJBs):

Knowledge Script	What It Does
EJBActivation	Returns counts and response times for activation and passivation of entity and stateful session beans.
EJBMessageDelivery	Returns the number of messages that were delivered, and that failed to be delivered, to message driven beans.
EJBMessageSession	Returns server session statistics for the message driven bean pool.
EJBMethodCalls	Returns counts and response times for bean method calls.
EJBPersistence	Returns counts and response times for entity bean loads and stores.
EJBPool	Returns statistics on pool usage for entity and stateless beans.

Notes

- Activation and passivation counts are supported; activation and passivation times are not.
- Load and store counts are supported; load and store times are not.

Health Knowledge Scripts

The following Knowledge Scripts monitor general availability or performance metrics of IBM WebSphere Application Server:

Knowledge Script	What It Does
Availability	Monitors the availability of the application server instance.
HealthCheck	Verifies that the server is running and can respond to requests.
RequestMetrics	Monitors the amount of time a node spent processing a request.
ServerCPU	Returns CPU utilization of the application server.
ServerScanLog	Scans the server's JVM log file(s) for lines matching a pattern. See also the SetServerLogPath Knowledge Script.

J2C Connection Pool Knowledge Scripts

The following Knowledge Scripts are focused on Java 2 Connectivity (J2C) connection pools and are only applicable to version 5 of IBM WebSphere Application Server:

Knowledge Script	What It Does
J2CUsage	Returns connection usage statistics.
J2CWaits	Returns statistics regarding how many clients are waiting for connections, and how long those clients have to wait.

JDBC Connection Pool Knowledge Scripts

The following Knowledge Scripts are focused on Java Database Connectivity (JDBC) connection pools:

Knowledge Script	What It Does
JDBCDriver	Returns the amount of time, in seconds, that the JDCB data source spent running in the JDBC driver, which includes time spent in the JDBC driver, network, and database.
JDBCUsage	Returns connection usage statistics.
JDBCWaits	Returns the amount of time, in seconds, that a JDBC data source spent waiting for a Java Database Connectivity (JDBC) connection.

JVM Runtime Knowledge Scripts

The following Knowledge Scripts are focused on the Java Virtual Machine (JVM) runtime:

Knowledge Script	What It Does
JVMGCStats	Returns garbage collection statistics, including the count and duration of garbage collections.
JVMHeap	Returns memory help usage statistics.
JVMLocks	Returns the number of waits for a lock that have occurred, and the average wait time.
JVMObjects	Returns object creation and deletion statistics.
JVMThreads	Returns thread creation and destruction statistics.

These Knowledge Scripts require the JVM interface to be running.

Object Request Broker Knowledge Scripts

The following Knowledge Scripts are focused on the Object Request Broker (ORB):

Knowledge Script	What It Does
ORBInterceptor	Returns the processing time for each ORB interceptor.
ORBRequests	Returns ORB request statistics, including the average object reference lookup time, the number of requests received, and the average number of concurrent requests.

Reporting Knowledge Script

The following report is focused on IBM WebSphere Application Server:

Knowledge Script	What It Does
Report_HealthSummary	Reports the availability and response time characteristics of one or more IBM WebSphere Application Servers.

Session Manager Knowledge Scripts

The following Knowledge Scripts are focused on the Session Manager:

Knowledge Script	What It Does
SessionErrors	Returns information about session errors that have occurred.
SessionInvalid	Returns statistics related to session invalidations.
SessionLifetime	Returns statistics related to session lifetime.

Thread Pool Knowledge Script

The following Knowledge Script is focused on thread pools:

Knowledge Script	What It Does
ThreadPoolUsage	Returns various thread pool statistics, including the number of threads created and destroyed, the number of active threads, the thread pool size, and the percentage of time that all threads in the pool are in use.

Transaction Manager Knowledge Scripts

The following Knowledge Scripts are focused on the Transaction Manager:

Knowledge Script	What It Does
TransactionCommits	Returns statistics about the number of local and global transactions committed, rolled back, and timed out.
TransactionDuration	Returns statistics about the duration of local and global transaction prepares and commits.

Web Application and Servlet Knowledge Scripts

The following Knowledge Scripts are focused on Web applications and servlets:

Knowledge Script	What It Does
ServletErrors	Returns the number of errors that have occurred while servicing requests.
ServletRequests	Returns statistics on the number of requests made, and the response time for servicing those requests.
WebAppLoads	Returns the number of servlets that were loaded and reloaded.

Web Services Gateway Knowledge Script

The following Knowledge Script is focused on the Web services gateway:

Knowledge Script	What It Does
WSGWRequests	Returns the number synchronous and asynchronous requests received and responses sent.

Workload Manager Knowledge Scripts

The following Knowledge Scripts are focused on the Workload Manager:

Knowledge Script	What It Does
WLMClientRequests	Returns the number of outgoing requests, and the average response time to service those requests.
WLMServerRequests	Returns the number of incoming requests of various types, and the average number of concurrent requests.

Availability

Use this Knowledge Script to monitor the availability of IBM WebSphere Application Server. This script monitors the availability of the application server instance.

Resource Object

IBM WebSphere Application Server

Default Schedule

The default interval for this script is **Every 15 Minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if the server is down. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Event severity when application server is not running	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.

DynamicCacheEviction

Use this Knowledge Script to monitor cache entry evictions (invalidations). The script records the following data:

- The number of cache entries evicted from memory by a Least Recently Used (LRU) algorithm. These entries are written to disk if disk overflow is enabled.
- The number of cache entries evicted from memory and/or disk because their timeout expired.
- The number of cache entries explicitly invalidated from memory.
- The number of cache entries explicitly invalidated from disk.

You can set this script to raise an event if the number of cache entries evicted from memory exceeds a specified threshold. Excessive eviction of memory cache entries can point to a need to increase the memory cache size.

Resource Object

Dynamic Cache

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual templates? (y/n)	Set to **n** to disable collection of data and event triggering for individual cache templates, so that only aggregate data for all cached templates is processed. The default is y. **Note** If you run this Knowledge Script on an individual template (rather than on the Dynamic Cache node) and this parameter is set to n, the script will not perform any actions.
LRU evictions threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of LRU evictions exceeds this threshold, an event is raised. The default is -1.
Event severity when LRU evictions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of LRU evictions exceeds the threshold. The default is 25.

Timeout evictions threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of timeout evictions exceeds this threshold, an event is raised. The default is -1.
Event severity when timeout evictions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of timeout evictions exceeds the threshold. The default is 25.

DynamicCacheHits

Use this Knowledge Script to monitor the dynamic cache hit/miss statistics. The dynamic cache is used to cache servlet and JSP results, Web services, and IBM WebSphere Application Server commands and patterns. This script records the number of hits in memory, the number of hits on disk, and the number of misses (object not found in memory or disk cache). You can set a threshold on the cache hit ratio, which is the number of cache hits (disk plus memory) divided by the total number of hits and misses, expressed as a percentage.

Resource Object

Dynamic Cache

Default Schedule

The default interval for this script is **Every 15 Minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if the average hit ratio (expressed as a percentage) falls below the threshold. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual templates? (y/n)	Set to **n** to disable collection of data and event triggering for individual cache templates, so that only aggregate data for all cached templates is processed. The default is y. **Note** If you run this Knowledge Script on an individual template (rather than on the Dynamic Cache node) and this parameter is set to n, the script will not perform any actions.
Cache hit ratio threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the average hit ratio (expressed as a percentage) falls below this threshold, an event is raised. The default is -1.
Event severity when cache hit ratio falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

EJBActivation

Use this Knowledge Script to monitor Enterprise Java Bean (EJB) activation rates. The script reports on the number of EJB activations and passivations, and the average amount of time required to activate and passivate an EJB. This script applies only to entity and stateful session EJBs.

Note
To discover EJB objects, an application running EJB must be available when you run the Discovery_WebSphereAppSrvUNIX Knowledge Script.

Resource Object

Enterprise Java Beans node or a stateful EJB module

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual EJB modules? (y/n)	Set to **n** to aggregate event and data details for the EJB modules that belong to an Enterprise Java Beans node. The default is y. If you run this script on a particular EJB module, rather than on the Enterprise Java Beans node, and this parameter is set to **n**, the script will not perform any actions unless the **Include results for individual EJBs** parameter is set to y.
Include results for individual EJBs? (y/n)	Set to **n** to disable collection of data and event triggering for individual EJBs, so that only aggregate data for the EJB module or Enterprise Java Bean collection is included. The default is y. **Note** If you run this Knowledge Script on an individual EJB (rather than on the Enterprise Java Beans node, or on an EJB module) and this parameter is set to n, the script will not perform any actions.
Activations threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of EJB activations exceeds this threshold, an event is raised. The default is -1.
Event severity when activations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of EJB activations exceeds the threshold. The default is 25.
Passivations threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of EJB passivations exceeds this threshold, an event is raised. The default is -1.

Event severity when passivations exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of EJB passivations exceeds the threshold. The default is 25.
Average activation time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average activation time (in seconds) exceeds this threshold, an event is raised. The default is -1.
Event severity when average activation time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average activation time (in seconds) exceeds this threshold. The default is 25.
Average passivation time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average passivation time (in seconds) exceeds this threshold, an event is raised. The default is -1.
Event severity when average passivation time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the the average passivation time (in seconds) exceeds the threshold. The default is 25.

EJBMessageDelivery

Use this Knowledge Script to monitor Enterprise Java Bean (EJB) message delivery statistics, for message-driven beans only. The script records the number of message delivery attempts, such as calls to a EJB's `onMessage` method, and the number of successful attempts.

Note
To discover EJB objects, an application running EJB must be available when you run the Discovery_WebSphereAppSrvUNIX Knowledge Script.

Resource Object

Enterprise Java Beans node or a message-driven EJB module

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if the percent of messages that failed to be delivered exceeds the threshold. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual EJB modules? (y/n)	Set to **n** to aggregate event and data details for the EJB modules that belong to an Enterprise Java Beans node. The default is y. If you run this script on a particular EJB module, rather than on the Enterprise Java Beans node, and this parameter is set to **n**, the script will not perform any actions unless the **Include results for individual EJBs** parameter is set to y.
Include results for individual EJBs? (y/n)	Set to **n** to disable collection of data and event triggering for individual EJBs, so that only aggregate data for the EJB module or Enterprise Java Bean collection is included. The default is y. **Note** If you run this Knowledge Script on an individual EJB (rather than on the Enterprise Java Beans node, or on an EJB module) and this parameter is set to n, the script will not perform any actions.
Failed message delivery percent threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the percent of messages that failed to be delivered exceeds this threshold, an event is raised. The default is -1.
Event severity when failed message delivery percent exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

EJBMessageSession

Use this Knowledge Script to monitor the server session pool used by message-driven Enterprise Java Beans (EJBs). The script records the average time to retrieve a ServerSession from the pool, and the percentage of the server session pool that is in use.

Note
To discover EJB objects, an application running EJB must be available when you run the Discovery_WebSphereAppSrvUNIX Knowledge Script.

Resource Object

Enterprise Java Beans node or a message-driven EJB module

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual EJB modules? (y/n)	Set to **n** to aggregate event and data details for the EJB modules that belong to an Enterprise Java Beans node. The default is y. If you run this script on a particular EJB module, rather than on the Enterprise Java Beans node, and this parameter is set to **n**, the script will not perform any actions unless the **Include results for individual EJBs** parameter is set to y.
Include results for individual EJBs? (y/n)	Set to **n** to disable collection of data and event triggering for individual EJBs, so that only aggregate data for the EJB module or Enterprise Java Bean collection is included. The default is y. **Note** If you run this Knowledge Script on an individual EJB (rather than on the Enterprise Java Beans node, or on an EJB module) and this parameter is set to n, the script will not perform any actions.
Average wait time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average wait time (in seconds) to obtain a server session exceeds this threshold, an event is raised. The default is -1.
Event severity when average wait time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average wait time (in seconds) to obtain a server session exceeds the threshold. The default is 25.

Server session pool usage threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the average percentage of the server session pool in use exceeds this threshold, an event is raised. The default is -1.
Event severity when server session pool usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average percentage of the server session pool in use exceeds the threshold. The default is 25.

EJBMethodCalls

Use this Knowledge Script to monitor Enterprise Java Bean (EJB) method call rates. The script reports on the number of EJB method calls, the current number of active methods, and the average amount of time required for each method call. This script applies to all EJBs.

Note
To discover EJB objects, an application running EJB must be available when you run the Discovery_WebSphereAppSrvUNIX Knowledge Script.

Resource Object

Enterprise Java Beans node or a single entity EJB module

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if the average time (in seconds) to complete a method call exceeds the threshold. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual EJB modules? (y/n)	Set to **n** to aggregate event and data details for the EJB modules that belong to an Enterprise Java Beans node. The default is y. If you run this script on a particular EJB module, rather than on the Enterprise Java Beans node, and this parameter is set to **n**, the script will not perform any actions unless the **Include results for individual EJBs** parameter is set to y.
Include results for individual EJBs? (y/n)	Set to n to disable collection of data and event triggering for individual EJBs, so that only aggregate data for the EJB module or Enterprise Java Bean collection is included. The default is y. **Note** If you run this Knowledge Script on an individual EJB (rather than on the Enterprise Java Beans node, or on an EJB module) and this parameter is set to n, the script will not perform any actions.
Average method call time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average time (in seconds) to complete a method call exceeds this threshold, an event is raised. The default is -1.
Event severity when average method call time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

EJBPersistence

Use this Knowledge Script to monitor Enterprise Java Bean (EJB) persistence (load and store) rates. The script reports on the number of EJB loads and stores, and the average amount of time required to load and store an EJB. This script applies only to entity EJBs.

Note
To discover EJB objects, an application running EJB must be available when you run the Discovery_WebSphereAppSrvUNIX Knowledge Script.

Resource Object

Enterprise Java Beans node or a single entity EJB module

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual EJB modules? (y/n)	Set to **n** to aggregate event and data details for the EJB modules that belong to an Enterprise Java Beans node. The default is y. If you run this script on a particular EJB module, rather than on the Enterprise Java Beans node, and this parameter is set to **n**, the script will not perform any actions unless the **Include results for individual EJBs** parameter is set to y.
Include results for individual EJBs? (y/n)	Set to **n** to disable collection of data and event triggering for individual EJBs, so that only aggregate data for the EJB module or Enterprise Java Bean collection is included. The default is y. **Note** If you run this Knowledge Script on an individual EJB (rather than on the Enterprise Java Beans node, or on an EJB module) and this parameter is set to n, the script will not perform any actions.
Loads threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of EJB loads exceeds this threshold, an event is raised. The default is -1.
Event severity when loads exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of EJB loads exceeds the threshold. The default is 25.
Stores threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of EJB stores exceeds this threshold, an event is raised. The default is -1.

Event severity when stores exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of EJB stores exceeds the threshold. The default is 25.
Average load time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average load time (in seconds) exceeds this threshold, an event is raised. The default is -1.
Event severity when average load time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average load time (in seconds) exceeds this threshold. The default is 25.
Average store time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average store time (in seconds) exceeds this threshold, an event is raised. The default is -1.
Event severity when average store time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average store time (in seconds) exceeds the threshold. The default is 25.

EJBPool

Use this Knowledge Script to monitor Enterprise Java Bean (EJB) pool usage statistics for entity and stateless session beans. This script monitors:

- The number of calls retrieving an object from the pool.
- The number of times a retrieve found an object available in the pool.
- The number of calls returning an object to the pool.
- The number of times the returned object was discarded because the pool was full.

Note
To discover EJB objects, an application running EJB must be available when you run the Discovery_WebSphereAppSrvUNIX Knowledge Script.

Resource Object

Enterprise Java Beans node, or a single entity or stateless session EJB module

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual EJB modules? (y/n)	Set to **n** to aggregate event and data details for the EJB modules that belong to an Enterprise Java Beans node. The default is y. If you run this script on a particular EJB module, rather than on the Enterprise Java Beans node, and this parameter is set to **n**, the script will not perform any actions unless the **Include results for individual EJBs** parameter is set to y.
Include results for individual EJBs? (y/n)	Set to **n** to disable collection of data and event triggering for individual EJBs, so that only aggregate data for the EJB module or Enterprise Java Bean collection is included. The default is y. **Note** If you run this Knowledge Script on an individual EJB (rather than on the Enterprise Java Beans node, or on an EJB module) and this parameter is set to n, the script will not perform any actions.
Successful retrieval percent threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the percent of retrievals that found an object available in the pool falls below this threshold, an event is raised. The default is -1.

Event severity when successful retrieval percent falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percent of retrievals that found an object available in the pool falls below the threshold. The default is 25.
Successful return percent threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the percent of returned objects that were not discarded because the pool was full falls below this threshold, an event is raised. The default is -1.
Event severity when successful return percent falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percent of returned objects that were not discarded because the pool was full falls below this threshold. The default is 25.

HealthCheck

Use this Knowledge Script to verify that IBM WebSphere Application Server is running, and that a user-specified servlet running on the server is able to respond to requests. You can specify that an event be raised if the servlet response time exceeds a specified threshold. You can also specify that the server should be restarted if it is not running.

In order to test for the application server's ability to respond to requests, and to measure the server's responsiveness, you must supply the URL of a servlet to query. In addition, you can optionally specify a string expected to be found in the document returned from the query. The URL must be an HTTP URL, and must be a GET, and not a POST, request. It is not required that the URL point to the local computer on which the health check is being performed, nor is it required that the URL point to a servlet. However, querying a remote URL will effectively check the health of the remote server, rather than the server on which the Knowledge Script runs. This may be useful in cases where you want to measure the response time of a servlet running on one server from the point of view of one or more other servers.

If security is enabled on the IBM WebSphere Application Server, you must use AppManager Security Manager to update the AppManager repository to provide the IBM WebSphere Application Server account information that is required to start the application server.

Resource Object

IBM WebSphere Application Server

Default Schedule

The default interval for this script is **Every 15 Minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Event severity when the application server is not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the application server is not running. The default is 10.
Restart application server if not running? (y/n)	Set to **y** to restart the application server if it is not running. The default is n.
Start time limit	Set to the number of seconds within which IBM WebSphere Application Server should complete initialization. The default is 300.
URL of servlet to test server responsiveness	Specify an HTTP GET URL to be accessed in order to test whether the server is able to respond to requests in a timely manner. Leave blank if you do not want to test server responsiveness.
Event severity when the servlet is not responding to requests	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the servlet is not responding to requests. The default is 10.

Text expected to be found in servlet response	Specify a string that should be found in the response text returned by the servlet. You can specify that an event be raised if this text is not found in the response. Leave this field empty if you do not want to validate the servlet response.
Event severity when text not found in servlet response	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the servlet response does not include the text you specify. The default is 25.
Servlet response time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the response time (in seconds) exceeds this threshold, an event is raised. The default is -1.
Event severity when servlet response time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the response time (in seconds) exceeds this threshold. The default is 25.

J2CUsage

Use this Knowledge Script to monitor the J2C (Java 2 Connectivity) connection pool usage statistics. The script records the following data:

- The average percentage of the pool that is in use.
- The average percentage of the time that all connections in the pool are in use.
- The average time, in seconds, that a connection is in use.
- The number of ManagedConnection objects that are in use.
- The number of connection handles that are in use.

Resource Object

J2C Connection Pool, or a J2C Data Source on version 5 of IBM WebSphere Application Server. This Knowledge Script is not applicable on version 6 of IBM WebSphere Application Server.

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if the percentage of the pool that is in use falls below the threshold. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual data sources? (y/n)	Set to **n** to disable collection of data and event triggering for individual data sources, so that only aggregate data for the provider or connection pool is processed. The default is y. **Note** If you run this Knowledge Script on an individual data source (rather than on the J2C Connection Pools node) and this parameter is set to n, the script will not perform any action.
Percent of pool in use threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the percentage of the pool that is in use falls below this threshold, an event is raised. The default is -1.
Event severity when percent of pool in use falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

J2CWaits

Use this Knowledge Script to monitor the time spent waiting for J2C (Java 2 Connectivity) connections. This script records the average number of threads concurrently waiting for connections, the average time spent waiting for a connection, and the number of faults (usually connection timeouts) that have occurred.

Resource Object

J2C Connection Pool or a J2C Data Source on version 5 of IBM WebSphere Application Server. This Knowledge Script is not applicable on version 6 of IBM WebSphere Application Server.

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual data sources? (y/n)	Set to **n** to disable collection of data and event triggering for individual data sources, so that only aggregate data for the provider or connection pool is processed. The default is y. **Note** If you run this Knowledge Script on an individual data source (rather than on the J2C Connection Pools node) and this parameter is set to n, the script will not perform any actions.
Threads currently awaiting a connection	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of threads currently waiting for a connection exceeds this threshold, an event is raised. The default is -1.
Event severity when threads currently awaiting a connection exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of threads currently waiting for a connection exceeds this threshold. The default is 25.
Average wait time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average time (in seconds) spent waiting for a connection exceeds this threshold, an event is raised. The default is -1.
Event severity when average wait time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average time (in seconds) spent waiting for a connection exceeds the threshold. The default is 25.

Connection faults	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of faults exceeds this threshold, an event is raised. The default is 0.
Event severity when connection faults exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of faults exceeds the threshold. The default is 25.

JDBCDriver

Use this Knowledge Script to monitor the amount of time, in seconds, that the JDCB data source spent running in the JDBC driver, which includes time spent in the JDBC driver, network, and database.

Resource Object

JDBC Connection Pool, or a JDBC Provider, or a JDBC Data Source

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if the amount of time (in seconds) spent executing in the JDBC driver exceeds the threshold. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual providers? (y/n)	Set to **n** to aggregate event and data details for individual providers, so that only aggregate data for the connection pool is processed. The default is y. If you run this Knowledge Script on an individual provider or data source (rather than on the JDBC Connection Pools node) and this parameter is set to n, the script will not perform any actions unless the **Include results for individual data sources** parameter is set to y.
Include results for individual data sources? (y/n)	Set to **n** to disable collection of data and event triggering for individual data sources, so that only aggregate data for the provider or connection pool is processed. The default is y. **Note** If you run this Knowledge Script on an individual data source (rather than on the JDBC Connection Pools node, or on a provider node) and this parameter is set to n, the script will not perform any actions.
Time spent executing in JDBC driver threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If amount of time (in seconds) spent executing in the JDBC driver exceeds this threshold, an event is raised. The default is -1.
Event severity when time spent in JDBC driver exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

JDBCUsage

Use this Knowledge Script to monitor the Java Database Connectivity (JDBC) connection pool usage statistics. The script records the following data:

- The average percentage of the pool that is in use.
- The average percentage of the time that all connections in the pool are in use.
- The average time a connection is in use.
- The number of ManagedConnection objects that are in use.
- The number of connection handles that are in use.

Resource Object

JDBC Connection Pool, or a JDBC Provider, or a JDBC Data Source

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if the current percent of the pool that is in use falls below the threshold. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual providers? (y/n)	Set to **n** to aggregate event and data details for individual providers, so that only aggregate data for the connection pool is processed. The default is y. If you run this Knowledge Script on an individual provider or data source (rather than on the JDBC Connection Pools node) and this parameter is set to n, the script will not perform any actions unless the **Include results for individual data sources** parameter is set to y.
Include results for individual data sources? (y/n)	Set to **n** to disable collection of data and event triggering for individual data sources, so that only aggregate data for the provider or connection pool is processed. The default is y. **Note** If you run this Knowledge Script on an individual data source (rather than on the JDBC Connection Pools node, or on a provider node) and this parameter is set to n, the script will not perform any actions.
Current percent of pool in use threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the current percent of the pool that is in use falls below this threshold, an event is raised. The default is -1.
Event severity when current percent of pool in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

JDBCWaits

Use this Knowledge Script to monitor the amount of time, in seconds, that a JDBC data source spent waiting for a Java Database Connectivity (JDBC) connection. This script records the number of threads currently waiting for connections, the average time spent waiting for a connection, and the number of faults (usually connection timeouts) that have occurred.

Resource Object

JDBC Connection Pool, or a JDBC Provider, or a JDBC Data Source

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual providers? (y/n)	Set to **n** to aggregate event and data details for individual providers, so that only aggregate data for the connection pool is processed. The default is y. **Note** If you run this Knowledge Script on an individual provider or data source (rather than on the JDBC Connection Pools node) and this parameter is set to n, the script will not perform any actions unless the **Include results for individual data sources** parameter is set to y.
Include results for individual data sources? (y/n)	Set to **n** to disable collection of data and event triggering for individual data sources, so that only aggregate data for the provider or connection pool is processed. The default is y. **Note** If you run this Knowledge Script on an individual data source (rather than on the JDBC Connection Pools node, or on a provider node) and this parameter is set to n, the script will not perform any actions.
Threads currently awaiting a connection threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of threads currently waiting for a connection exceeds this threshold, an event is raised. The default is -1.
Event severity when threads currently awaiting a connection exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threads currently awaiting a connection exceed the threshold. The default is 25.
Average wait time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average time (in seconds) spent waiting for a connection exceeds this threshold, an event is raised. The default is -1.

Event severity when average wait time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average time (in seconds) spent waiting for a connection exceeds the threshold. The default is 25.
Connection faults threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of faults exceeds this threshold, an event is raised. The default is 0.
Event severity when connection faults exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of faults exceeds the threshold. The default is 25.

JVMGCStats

Use this Knowledge Script to monitor garbage collection statistics for objects in the Java Virtual Machine (JVM) heap. This script records the number of garbage collections, the average time between collections, and the average collection duration.

This Knowledge Script requires the JVM interface to be running.

Resource Object

JVM Runtime

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Garbage collections threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of garbage collections exceeds this threshold, an event is raised. The default is -1.
Event severity when garbage collections exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of garbage collections exceeds the threshold. The default is 25.
Average garbage collection duration threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average garbage collection duration (in seconds) exceeds this threshold, an event is raised. The default is -1.
Event severity when average garbage collection duration exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average garbage collection duration (in seconds) exceeds the threshold. The default is 25.
Average time between calls threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average time (in seconds) between calls false below this threshold, an event is raised. The default is -1.
Event severity when average time between calls falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average time (in seconds) between calls false below the threshold. The default is 25.

JVMHeap

Use this Knowledge Script to monitor memory usage statistics of the application server's Java Virtual Machine (JVM) heap. This script reports the amount of free and used heap memory.

This Knowledge Script requires the JVM interface to be running.

Resource Object

JVM Runtime

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise event if a threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Heap size threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the current size of the heap in KB exceeds this threshold, an event is raised. The default is -1.
Event severity when heap size exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the current size of the heap in KB exceeds the threshold. The default is 25.
Free heap threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of KB available in the heap falls below this threshold, an event is raised. The default is -1.
Event severity when free heap falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of KB available in the heap falls below the threshold. The default is 25.
Percent heap used threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the percentage of the JVM heap that is currently used exceeds this threshold, an event is raised. The default is -1.
Event severity percent heap used exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of the JVM heap that is currently used exceeds the threshold. The default is 25.

JVMLocks

Use this Knowledge Script to monitor Java Virtual Machine (JVM) lock statistics. This script records the number of times a thread waits for a lock, and the average wait time for a lock.

This Knowledge Script requires the JVM interface to be running.

Resource Object

JVM Runtime

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Lock waits threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the average number of lock waits exceeds this threshold, an event is raised. The default is -1.
Event severity when lock waits exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average number of lock waits exceeds the threshold. The default is 25.
Average lock wait duration threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average duration of the wait for a lock (in seconds) exceeds this threshold, an event is raised. The default is -1.
Event severity when average lock wait duration exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average duration of the wait for a lock (in seconds) exceeds the threshold. The default is 25.

JVMObjects

Use this Knowledge Script to monitor allocation statistics for objects in the Java Virtual Machine (JVM) heap. This script records the number of objects allocated, moved, and freed in the heap.

This Knowledge Script requires the JVM interface to be running.

Resource Object

JVM Runtime

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Objects allocated threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of objects allocated exceeds this threshold, an event is raised. The default is -1.
Event severity when objects allocated exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of objects allocated exceeds the threshold. The default is 25.
Objects moved threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of objects moved exceeds this threshold, an event is raised. The default is -1.
Event severity when objects moved exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of objects moved exceeds the threshold. The default is 25.
Objects freed threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of objects freed exceeds this threshold, an event is raised. The default is -1.
Event severity when objects freed exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of objects freed exceeds the threshold. The default is 25.

JVMThreads

Use this Knowledge Script to monitor Java Virtual Machine (JVM) thread creation and destruction. The script records the number of threads that start executing, and the number that finish executing.

This Knowledge Script requires the JVM interface to be running.

Resource Object

JVM Runtime

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if the average number of threads started exceeds this threshold. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Threads started threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the average number of threads started exceeds this threshold, an event is raised. The default is -1.
Event severity when threads started exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

NetIQAgent

Use this Knowledge Script to start or stop the Java server that the AppManager managed object uses to communicate with IBM WebSphere Application Server. This Java server must be running in order for WebSphere Application Server Knowledge Scripts to work properly.

Typically, you do not need to manually start or stop the Java server. The Java server starts automatically when you discover IBM WebSphere Application Server.

If you encounter problems with WebSphere Application Server Knowledge Scripts collecting performance data, use this Knowledge Script to stop and restart the Java server.

When you discover IBM WebSphere Application Server, you specify the port that the Java server uses to communicate with the managed object. You can use this Knowledge Script to update the communication port on the Java server without rediscovering IBM WebSphere Application Server. To change the listening port for the Java server, you must stop and restart the Java server to apply your changes.

Resource Object

IBM WebSphere Application Server

Default Schedule

The default interval for this script is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if the Java server cannot be started or stopped. The default is y.
Event severity when agent cannot be started or stopped	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Start agent? (y/n)	Set to **y** to start the agent, or **n** to stop the agent. The default is y.
TCP port	Specify the TCP port to be used by the Java server when listening for requests. The same port should normally be specified for all computers on which the Java server runs. However, this is strictly required only if you intend to run the RequestMetrics Knowledge Script. The default TCP port is 4000.

ORBInterceptor

Use this Knowledge Script to monitor the processing time for each Object Request Broker (ORB) interceptor.

Resource Object

ORB, or an individual ORB interceptor

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if the time (in seconds) spent executing in the interceptor exceeds the threshold. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual ORB interceptors? (y/n)	Set to **n** to disable collection of data and event triggering for individual interceptors, so that only aggregate data for the ORB is processed. The default is y. **Note** If you run this Knowledge Script on an individual interceptor (rather than on the Object Request Broker node) and this parameter is set to **n**, the script will not perform any actions.
Processing time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the time (in seconds) spent executing in the interceptor exceeds this threshold, an event is raised. The default is -1.
Event severity when processing time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

ORBRequests

Use this Knowledge Script to monitor Object Request Broker (ORB) request statistics. This script records the average object reference lookup time, the number of requests received, and the average number of concurrent requests.

Resource Object

ORB

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Average reference lookup time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average time (in seconds) to look up an object reference exceeds this threshold, an event is raised. The default is -1.
Event severity when average reference lookup time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average time (in seconds) to look up an object reference exceeds the threshold. The default is 25.
Requests received threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of requests received exceeds this threshold, an event is raised. The default is -1.
Event severity when requests received exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of requests received exceeds the threshold. The default is 25.
Concurrent requests threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of requests currently being processed exceeds this threshold, an event is raised. The default is -1.
Event severity when concurrent requests exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of requests currently being processed exceeds this threshold. The default is 25.

Report_HealthSummary

Use this Knowledge Script to generate a report showing the availability and response time characteristics of one or more WebSphere Application Servers. The availability and response time measurements are based on the results generated by running the HealthCheck Knowledge Script, so no results will be available if that script has not been run. The response time measurements are based on the response times produced by the servlet specified in the HealthCheck Knowledge Script. If you run this report against multiple servers for which different servlets were specified in HealthCheck jobs, the response time metrics for the servers may not be directly comparable.

Resource Object

WebSphereAppSrvUNIX sub-node of Report Agent node

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Select the IBM WebSphere Application Servers. Click **Browse [...]** to select from one to twenty-five views. Your subsequent selections are limited to computers or server groups that are visible in the selected views. Select one of the Filters options: **View:** Includes all computers in the views you selected. **Computer:** Select from individual computers in the views you selected. **Server Group:** Select from server groups in the views you selected. Selecting a server group includes all computers in that group.
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.
Aggregation by	Select the time period (Hour, Minute, or Day) by which the data in your report is aggregated. The default is Hour.
Aggregation interval	Select the interval between aggregations of the data in your report. This parameter uses the time period specified in the **Aggregation by** parameter to calculate the interval. The default is 1.
Report component selection	
Include parameter card?	Set to **y** to include a table showing report parameters. The default is y.
Include Running detail table?	Set to **y** to include a table of Running results (whether the server was found to be running) in the report. The default is y.

Include Running chart?	Set to **y** to include a chart of Running results (whether the server was found to be running) in the report. The default is y.
Threshold on Running chart	Specify the threshold to be shown on the Running chart. Use -1 to indicate that no threshold is to be shown.
Include Servlet Response Time detail table?	Set to **y** to include table of Servlet Response Time results in the report. The default is y.
Include Servlet Response Time chart?	Set to **y** to include chart of Servlet Response Time results in the report. The default is y.
Units for Servlet Response Time chart	Specify the units to be used for the Servlet Response Time chart. The default is milliseconds.
Threshold on Servlet Response Time chart	Specify the threshold to be shown on the Servlet Response Time chart. Use -1 to indicate that no threshold is to be shown.
Report settings	
Customize chart appearance	Specify the type and attributes of chart(s) to be generated. A wide selection of chart types is available. The default is Ribbon.
Select report location	Choose the report filename. The default is WebSphereAppSrvUNIX_HealthSummary.
Add job ID to output folder name?	Set to **y** to include the report job ID to the report output folder name. The default is n.
Index-report Title	Choose the report title, author, company, component, description, expiration period, and custom fields. Defaults are: Title = WebSphereAppSrvUNIX Health Summary Author = NetIQ AppManager Company = Your company here Component = NetIQ AppManager 5.0 <Module> Description = WebSphereAppSrvUNIX Health Summary: Availability and Servlet Response Time. Expiration Period = Expires after 7 days Custom Field 1 = WebSphereAppSrv, UNIX, Health Summary Custom Field 2 = Availability and Servlet Response Time
Add time stamp to title	Set to **y** to include the time the report was generated in the report title. The default is n.
Event notification	
Generate event on success?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Severity level for report success	Specify a severity level for the event raised when the report is generated successfully. The default is 35.
Severity level for report with no data	Specify a severity level for the event raised when no data for the report is found within the selected time interval. The default is 25.
Severity level for report failure	Specify a severity level for the event raised when the report generation fails. The default is 5.

RequestMetrics

Use this Knowledge Script to monitor the amount of time a node spent processing a request. In a multi-node deployment, requests typically enter the system and create processes that fan out across several nodes within the distributed system. Use this script to gather and correlate data collected at each node of the system, in order to provide a breakdown of how much time is spent in different components of the request-processing pipeline.

Before using this Knowledge Script, you must run the SetRMFilters script to instruct IBM WebSphere Application Server to collect metrics for requests that match a given set of patterns, such as client IP address, URL, or EJB method names. Once request metrics are enabled, IBM WebSphere Application Server will write an entry to the trace log each time a matching HTTP request is received or a remote EJB method call is made. This script can then be used to gather and correlate these trace log entries.

In order for this script to gather request metrics, it must be provided with a list of the hosts from which data is to be collected. Normally, you should specify all hosts in the IBM WebSphere Application Server domain, but you can restrict the data to a particular subset of nodes by specifying only those computers. You do not need to specify individual application servers on the selected computers-the log files for all of the known application servers on each computer will be analyzed.

This script measures the request-processing time for only those requests that entered the system at the node on which this script is run. Any request that enters the IBM WebSphere Application Server network at an upstream node is ignored. Hence, run this script only on the node containing the entry point for request processing. This script can be set to raise an event if the average request-processing response time exceeds a specified threshold. The detail message associated with the event shows the breakdown of how much time was spent in each component. You can also specify that a data stream containing the average response time be written to the database.

Resource Object

IBM WebSphere Application Server

Default Schedule

The default interval for this script is **Every 15 Minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Semicolon-separated list of hosts from which to collect data	Specify the hosts from which request metrics data should be gathered. Normally, you should specify all hosts in the IBM WebSphere Application Server domain.
Request-processing time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average time to process a request (in seconds) exceeds this threshold, an event is raised. The default is -1.
Event severity when the request-processing time exceeds the threshold?	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

ServerCPU

Use this Knowledge Script to monitor the CPU utilization of the application server. On multiprocessor systems, the CPU utilization is the average over all CPUs.

Resource Object

IBM WebSphere Application Server

Default Schedule

The default interval for this script is **Every 15 Minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Average CPU utilization threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the CPU utilization of IBM WebSphere Application Server exceeds this threshold, an event is raised. The default is 90.
Event severity when average CPU utilization exceeds threshold	Set the event severity level, from 1 to 40, to indicate event importance. The default is 25.

ServerScanLog

Use this Knowledge Script to monitor the server's primary Java Virtual Machine (JVM) log file. The script scans the log file for any lines written since the last iteration of the script that match the given *inclusion* filter and do not match the given *exclusion* filter. If the number of lines that pass this filtering exceeds a specified threshold, an event is raised. The detailed message associated with the event contains the matching lines.

The inclusion and exclusion filters are Perl regular expressions. Because the application server writes log entries in a specific format, a simple inclusion filter can be used to scan for errors of a specific type. For example, to scan for error entries, use an exclusion filter of `"\sE\s"`. For fatal errors, replace 'E' with 'F'. For warnings, use 'W'.

In addition to raising an event when a threshold is exceeded, this script records a data stream for the number of matching lines.

Resource Object

IBM WebSphere Application Server

Default Schedule

The default interval for this script is **Every 15 Minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Event severity when the log file does not exist	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 20.
Log entries matched threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of log entries that match the search criteria exceeds this threshold, an event is raised. The default is 0.
Event severity when log entries matched exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Inclusion filter	Set to a string that is a Perl regular expression. Lines matching this expression pass the filter unless they also match the exclusion filter. The default is a null string.
Ignore case in inclusion filter matching? (y/n)	Set to **y** to ignore case when matching lines against the inclusion filter. The default is n.
Exclusion filter	Set to a string that is a Perl regular expression. Lines matching this expression are never returned, even if they pass the inclusion filter. The default is a null string.
Ignore case in exclusion filter matching? (y/n)	Set to **y** to ignore case when matching lines against the exclusion filter. The default is n.

ServletErrors

Use this Knowledge Script to monitor errors generated by a servlet, or by the N servlets with the highest, or lowest, number of errors.

Resource Object

Web application or servlet

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Number of servlets	Specify the number of servlets for which data should be collected. Use -1 (or 0) to indicate that all servlets should be processed. The default is 5.
Sort order	Set to **descending** to sort the servlets in decreasing order. Set to **ascending** to sort in ascending order. The default is descending.
Errors threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of errors exceeds this threshold, an event is raised. The default is 0.
Event severity when errors exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

ServletRequests

Use this Knowledge Script to monitor servlet requests and response times. This script records the number of requests received, the number of concurrent requests, and the average time taken to service a request. You can run this script against a single servlet, or you can run it against a Web application to get results for the servlets with the worst, or best, value for a specified performance metric.

Resource Object

Web application or servlet

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Number of servlets	Specify the number of servlets for which data should be collected. Use -1 (or 0) to collect data for all servlets. The default is 5.
Sort by	Specify the performance metric by which servlets are sorted. The default is Response Time.
Sort order	Set to **descending** to sort the servlets in decreasing order; set to **ascending** to sort in ascending order. The default is descending.
Requests received threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of requests received exceeds this threshold, an event is raised. The default is -1.
Event severity when requests received exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Concurrent requests threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of concurrent requests exceeds this threshold, an event is raised. The default is -1.
Event severity when concurrent requests exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Average request processing time threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average time (in seconds) required to service a request exceeds this threshold, an event is raised. The default is -1.
Event severity when average request processing time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

SessionErrors

Use this Knowledge Script to monitor the following HTTP session errors:

- Requests received for sessions that were last accessed from another Web application, which might indicate either failover processing or a corrupt plug-in configuration.
- Requests for a new session that could not be processed because the threshold for the maximum number of sessions is exceeded. This applies only to sessions in memory with `AllowOverflow = false`.

Resource Object

Session Manager

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is **y**.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Requests from unexpected source threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of requests from a different source than the most recent session request exceeds this threshold, an event is raised. The default is -1.
Event severity when requests from unexpected source exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
New session request failures threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of requests that fail because the session pool is full exceeds this threshold, an event is raised. The default is -1.
Event severity when new session requests failures exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

SessionInvalid

Use this Knowledge Script to monitor HTTP session invalidation statistics. This script records the following data:

- The number of sessions that were invalidated.
- The number of sessions that were invalidated due to a timeout.
- The number of requests for a session that no longer exists, presumably because the session timed out.

Resource Object

Session Manager

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Percent invalidated due to timeout threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the percent of invalidated sessions that were invalidated due to a timeout exceeds this threshold, an event is raised. The default is -1.
Event severity when percent invalidated due to timeout exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Requests for nonexistent session threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the average number of requests for sessions that do not exist exceeds this threshold, an event is raised. The default is -1.
Event severity when requests for nonexistent session exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

SessionLifetime

Use this Knowledge Script to monitor HTTP sessions. This script records the following data:

- The number of sessions created.
- The average lifetime of a session.
- The average number of active sessions.
- The number of live (cached in memory) sessions.

Resource Object

Session Manager

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Sessions created threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of sessions created exceeds this threshold, an event is raised. The default is -1.
Event severity when sessions created exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Average session lifetime threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If average session lifetime (in seconds) exceeds this threshold, an event is raised. The default is -1.
Event severity when average session lifetime exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Current active sessions threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the current number of active sessions exceeds this threshold, an event is raised. The default is -1.
Event severity when current active sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Current live sessions threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the current number of live sessions exceeds this threshold, an event is raised. The default is -1.
Event severity when current live sessions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

SetRMFilters

Use this Knowledge Script to specify the filters to be used for generating request metrics traces. You must specify filters using this script before you can collect response time data with the RequestMetrics Knowledge Script. Three types of filtering can be specified, as described below. In each case, the filter pattern is expressed as a string that can optionally contain an asterisk (*) as the last character. Matching is done character by character, until either an asterisk is found in the filter, a mismatch occurs, or an exact match occurs.

- URL filters: Requests are filtered based on the URL of the incoming HTTP request.
- Client IP address filters: Requests are filtered based on the IP address of the incoming HTTP request.
- EJB method name filters: Requests are filtered based on the full name of the enterprise bean method.

If both URL filters and client IP address filters are specified, a match occurs only if a filter of each type is matched. It is strongly suggested that at least one URL or client IP address filter be supplied, to avoid performance degradation due to the large number of trace records that otherwise would be written to the trace log.

If no filters are specified, this script turns off request metrics tracing altogether. That is, it has the effect of stopping request metrics tracing completely, rather than causing all requests to be traced. Thus, to turn on request metrics tracing, you must specify at least one filter. If you do not plan to run the RequestMetrics Knowledge Script on *any* computer in the IBM WebSphere Application Server domain for a long period of time, you can turn off tracing by specifying no filters to avoid the performance penalty engendered by writing request traces to the log file.

Note
In an IBM WebSphere Application Server network deployment, the Request Metrics configuration is managed centrally by the deployment manager, and the settings apply to all nodes and application servers in the cell. Therefore, you only need to run this Knowledge Script against a single server in the deployment cell.

Resource Object

IBM WebSphere Application Server

Default Schedule

The default interval for this script is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Semicolon-separated list of URL filters	Specify the URL patterns to be used in filtering. Patterns should be separated from one another by semicolons.

Semicolon-separated list of client IP address filters	Specify the IP address patterns to be used in filtering. Patterns should be separated from one another by semicolons.
Semicolon-separated list of EJB method name filters	Specify the EJB method name patterns to be used in filtering. Patterns should be separated from one another by semicolons.

SetServerLogPath

Use this Knowledge Script to specify the pathname of the server's primary Java Virtual Machine (JVM) log file. The JVM log contains messages written by the application server JVM itself, as well as by applications running within the server. If the JVM log file is being written to the default location, it is not necessary to run this script. However, if the JVM log file is being written to a different directory or has a different filename than the default, you must run this script before attempting to scan the log files using the ServerScanLog Knowledge Script. Failing to do so will cause ServerScanLog to raise an event when it is run.

In addition, to enable the RequestMetrics Knowledge Script to work properly, you must set the server log path because the RequestMetrics Knowledge Script collects traces from the server log file as well.

Resource Object

IBM WebSphere Application Server

Default Schedule

The default interval for this script is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Path name for WebSphere JVM log file	Specify the path to the server's primary JVM log file, SystemOut.log, either as an absolute path, or a path relative to the `WebSphere/AppServer` directory. Replace any spaces in the path name with an underscore.
Event severity when the log file does not exist	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 20.

StartServer

Use this Knowledge Script to start the IBM WebSphere Application Server. Starting an application server starts a server process based on the application server's configuration.

If WebSphere Application Server security is enabled, you must use AppManager Security Manager to update the AppManager repository to provide the IBM WebSphere Application Server account information that is required to start the application server.

Resource Object

IBM WebSphere Application Server

Default Schedule

The default interval for this script is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Event severity when application server cannot be started	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Event severity when application server is started successfully	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Start time limit	Set to the number of seconds within which the WebSphere Application Server should complete initialization. The default is 300.

StopServer

Use this Knowledge Script to stop the IBM WebSphere Application Server. Stopping an application server stops a server process based on the process definition settings in the current application server configuration.

If WebSphere Application Server security is enabled, you must use AppManager Security Manager to update the AppManager repository to provide the IBM WebSphere Application Server account information that is required to start the application server.

Resource Object

IBM WebSphere Application Server

Default Schedule

The default interval for this script is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Event severity when the server cannot be stopped	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15.
Event severity when the server is stopped successfully	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Stop time limit	Set to the number of seconds within which the WebSphere Application Server should stop running. The default is 300.

ThreadPoolUsage

Use this Knowledge Script to monitor thread pool activity. This script records the following:

- The number of threads created.
- The number of threads destroyed.
- The number of active threads.
- The thread pool size.
- The percentage of time that all threads in the pool are in use.

Resource Object

Thread Pools, or a particular thread pool

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Include results for individual thread pools? (y/n)	Set to **n** to disable collection of data and event triggering for individual thread pools, so that only aggregate data for all thread pools is processed. The default is y. **Note** If you run this Knowledge Script on an individual thread pool (rather than on the Thread Pools node) and this parameter is set to **n**, the script will not perform any actions.
Active threads threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of active threads exceeds this threshold, an event is raised. The default is -1.
Event severity when active threads exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Pool size threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the current pool size exceeds this threshold, an event is raised. The default is -1.
Event severity when pool size exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Percent of time all threads are in use threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the percentage of time that all threads in the pool are in use exceeds this threshold, an event is raised. The default is -1.
Event severity when percent of time all threads are in use exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

TransactionCommits

Use this Knowledge Script to monitor the number of commits, rollbacks and timeouts, for both local and global transactions.

Resource Object

Transaction Manager

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Global transaction commits threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of global transaction commits exceeds this threshold, an event is raised. The default is -1.
Event severity when global transaction commits exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Global transaction rollbacks threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of global transaction rollbacks exceeds this threshold, an event is raised. The default is -1.
Event severity when global transaction rollbacks exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Global transaction timeouts threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of global transaction timeouts exceeds this threshold, an event is raised. The default is -1.
Event severity when global transaction timeouts exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Local transaction commits threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of local transaction commits exceeds this threshold, an event is raised. The default is -1.
Event severity when local transaction commits exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Local transaction rollbacks threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of local transaction rollbacks exceeds this threshold, an event is raised. The default is -1.

Event severity when local transaction rollbacks exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Local transaction timeouts threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of local transaction timeouts exceeds this threshold, an event is raised. The default is -1.
Event severity when local transaction timeouts exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

TransactionDuration

Use this Knowledge Script to monitor the average transaction duration, as well as the duration of transaction prepares and commits, for both local and global transactions.

Resource Object

Transaction Manager

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Global transactions threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of global transactions exceeds this threshold, an event is raised. The default is -1.
Event severity when global transactions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Average global transaction duration threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average global transaction duration (in seconds) exceeds this threshold, an event is raised. The default is -1.
Event severity when average global transaction duration exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Local transactions threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of local transactions exceeds this threshold, an event is raised. The default is -1.
Event severity when local transactions exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Average local transaction duration threshold	Specify a threshold value greater than or equal to -1. Use -1 to ignore this threshold. If the average local transaction duration (in seconds) exceeds this threshold, an event is raised. The default is -1.
Event severity when average local transaction duration exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

WebAppLoads

Use this Knowledge Script to monitor the number of servlets loaded and reloaded for a particular Web application, or for the top N Web applications, sorted by a specified metric.

Resource Object

Web Applications, or a particular Web application

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Number of Web applications	Specify the number of Web applications for which data should be collected. Use –1 (or 0) to indicate that all Web applications should be processed.
Sort by	Specify the performance metric by which Web applications are sorted.
Sort order	Set to **descending** to sort the Web applications in decreasing order; set to **ascending** to sort in ascending order. The default is **descending**.
Servlets loaded threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of servlets loaded exceeds this threshold, an event is raised. The default is -1.
Event severity when servlets loaded exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Servlets reloaded threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of servlets reloaded exceeds this threshold, an event is raised. The default is -1.
Event severity when servlets reloaded exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

WLMClientRequests

Use this Knowledge Script to monitor the outgoing request-processing statistics for the Workload Manager. The script records the following data:

- The number of outgoing requests processed.
- The average response time required to service those requests.

Resource Object

Workload Manager (Client)

Default Schedule

The default interval for this script is **Every 15 minutes.**

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Outgoing requests threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of outgoing requests exceeds this threshold, an event is raised. The default is -1.
Request response time threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the average response time exceeds this threshold, an event is raised. The default is -1.
Event severity when request response time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

WLMServerRequests

Use this Knowledge Script to monitor the request-processing statistics for the Workload Manager. The script records the following data:

- The number of requests currently being processed.
- The number of requests processed.
- The average number of requests processed that have a strong affinity to the server. A strong affinity request is one that must be serviced by this application server because of a dependency that resides on the server. One example of this is transactional affinity.
- The average number of requests processed that do not have a strong affinity to the server.
- The average number of requests processed that came from a non-WLM enabled client, or were marked by the client not to participate in workload management.

Resource Object

Workload Manager Server

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Concurrent requests threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of concurrent requests exceeds this threshold, an event is raised. The default is -1.
Event severity when concurrent requests exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Strong affinity request percent threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the percent of requests that have a strong affinity to the server exceeds this threshold, an event is raised. The default is -1.
Event severity when strong affinity request percent exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

WSGWRequests

Use this Knowledge Script to monitor requests received and responses sent by a Web service.

Resource Object

Web Services or a particular Web service

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to **y** to raise events. The default is y.
Collect data? (y/n)	Set to **y** to collect data for reports and graphs. The default is n.
Synchronous requests received threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of synchronous requests received exceeds this threshold, an event is raised. The default is -1.
Event severity when synchronous requests received exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Synchronous responses sent threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of synchronous responses made exceeds this threshold, an event is raised. The default is -1.
Event severity when synchronous responses sent exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Asynchronous requests received threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of asynchronous requests received exceeds this threshold, an event is raised. The default is -1.
Event severity when asynchronous requests received exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Asynchronous responses sent threshold	Specify a threshold value using an integer greater than or equal to -1. Use -1 to ignore this threshold. If the number of asynchronous responses made exceeds this threshold, an event is raised. The default is -1.
Event severity when asynchronous responses sent exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.

Chapter 74
WebSphereMQUNIX Knowledge Scripts

The WebSphereMQUNIX category provides the following Knowledge Scripts for monitoring IBM WebSphere MQ Servers running on UNIX operating systems.

From in the Operator Console, you can select a Knowledge Script in the Knowledge Script pane and press **F1** for complete details.

Knowledge Script	What It Does
ADMINClearLocalQueue	Clears local queue messages.
ADMINQueueMgrStartStop	Sends a command to the WebSphere MQ Server to start or stop a queue manager.
ChannelStatus	Monitors the status of WebSphere MQ channels.
DynamicLocalQueueDepth	Monitors the depth of local queues, including dynamically created queues.
LocalQueueDepth	Monitors the total number of messages in discovered local queues.
PingQueueManager	Pings a local queue manager and restarts the command server or queue manager if either is detected down.
ServerDown	Monitors processes that belong to a specified WebSphere MQ Server user group.
TestQueueManager	Monitors the connection between the WebSphere MQ Server and a local queue manager.
WebSphereMQErrorLog	Monitors the WebSphere MQ error log file for specific strings and messages logged since the last monitoring interval.

ADMINClearLocalQueue

Use this Knowledge Script to clear local queue messages. This Knowledge Script clears the local queue of any messages when the local queue depth exceeds the specified threshold.

Alternatively, you can configure this Knowledge Script to clear the local queue each time the Knowledge Script job runs, regardless of how many messages are in the local queue.

An event is raised if the local queue cannot be cleared.

This Knowledge Script makes WebSphere MQ Server easier to administer because it can be used to clear several local queues at once.

Resource Object

MQSeries queue.

Default Schedule

The default interval for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Local queue depth threshold	Enter a threshold for the maximum number of messages in a local queue. If the threshold is exceeded, the local queue is cleared. The default is 5.
Clear all messages regardless of queue depth?	If set to **y**, a threshold cannot be set and all messages in the local queue are cleared, regardless of queue depth. The default is n.
Event severity if unable to clear queue	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

ADMINQueueMgrStartStop

Use this Knowledge Script to send a command to the WebSphere MQ Server to start or stop a queue manager. This Knowledge Script verifies that the command completed successfully.

An event is raised if the start or stop command completes successfully or if the command fails.

This Knowledge Script makes WebSphere MQ Server easier to administer, because it can start or stop several queue managers at once.

Resource Object

MQSeries queue manager.

Default Schedule

The default interval for this Knowledge Script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Start queue manager?	Set to **y** to start a queue manager. The default is y.
Stop queue manager?	Set to **y** to stop a queue manager. The default is n.
Time to wait before checking command results	Enter the length of time, in seconds, that the Knowledge Script should wait before attempting to confirm that a start or stop command completed successfully. When specifying this value, consider the following: • The system resources available to WebSphere MQ Server. • It takes longer to stop a queue manager than to start a queue manager. If the amount of time you specify is insufficient for the queue manager to start or stop, the status of the queue manager is not confirmed and an event is raised. The default is 30 seconds.
Event severity if command...	Set the event severity level, from 1 to 40, to indicate the importance if the command: ... **fails**. The default is 5 (red event indicator). ... **succeeds**. The default is 12 (yellow event indicator).

ChannelStatus

Use this Knowledge Script to monitor the status of WebSphere MQ channels. An event is raised when the channel is inactive, stopped, paused, or running.

If AppManager cannot retrieve the status of a channel because the channel is not initialized correctly, an event is raised and the event message includes a WebSphere MQ internal code describing the problem. You can use this information to locate the origin of the problem.

Resource Object

MQSeries channels.

Default Schedule

The default interval for this Knowledge Script is **Every 20 seconds** and **End after 3 times**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if channel is...	Set to **y** to raise an event if the channel status is: ... **inactive**. The default is y. ... **stopped**. The default is y. ... **paused**. The default is y. ... **running**. The default is n. ... **binding**. The default is n. ... **starting**. The default is n. ... **stopping**. The default is n. ... **retrying**. The default is n. ... **requesting**. The default is n. ... **initializing**. The default is n. ... **not found**. The default is n.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n. If set to **y**, the script returns a value of: • **100** if the channel is running. • **50** if the channel is binding, starting, stopping, retrying, requesting, or initializing. • **25** if channel is inactive, stopped, or paused. • **0** if the channel status cannot be retrieved.

Description	How to Set It
Event severity if channel...	Set the event severity level, from 1 to 40, to reflect the importance when the channel status is: ... **inactive**. Severity 5 (red event indicator). ... **stopped**. Severity 5 (red event indicator). ... **paused**. Severity 5 (red event indicator). ... **running**. Severity 25 (blue event indicator). ... **status cannot be retrieved**. Severity 25 (blue event indicator). ... **binding**. Severity 25 (blue event indicator). ... **starting**. Severity 25 (blue event indicator). ... **stopping**. Severity 25 (blue event indicator). ... **retrying**. Severity 25 (blue event indicator). ... **requesting**. Severity 25 (blue event indicator). ... **initializing**. Severity 25 (blue event indicator). ... **not found**. Severity 25 (blue event indicator).

DynamicLocalQueueDepth

Use this Knowledge Script to monitor the total number of messages in any specified local queue. If the number of messages in a queue exceeds the threshold you specify or the queue threshold specified in WebSphere MQ Explorer, an event is raised.

This Knowledge Script monitors an implementation of WebSphere MQ in which local queues are created and deleted dynamically. This Knowledge Script specifies queue names, does not raise events for queues that have already been deleted, and can monitor queues created since AppManager discovery was last run. For these reasons, the DynamicLocalQueueDepth Knowledge Script functions more efficiently than LocalQueueDepth for a dynamic implementation of WebSphere MQ.

If necessary, adjust the schedule to reflect the rate at which local queues are created and deleted.

Resource Object

MQSeries queue manager.

Default Schedule

The default interval is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Queue name search criteria	Enter the queue name you want to monitor. The asterisk can be used as a wildcard. For example, the default (SYS*) monitors all system local queues. Queue names are case-sensitive.
Use queue's own threshold?	Set to **y** to use the queue threshold defined in the queue's local attributes. An event is raised if the threshold is met or exceeded. The default is n.
Queue message depth threshold	If you prefer not to use the queue's own threshold, enter a threshold for the maximum number of messages in the local queues being monitored. An event is raised if the threshold is met or exceeded. The default is 5.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

LocalQueueDepth

Use this Knowledge Script to monitor the total number of messages in the local queues. If the number of queue messages exceeds the threshold, an event is raised. The threshold is defined by any or all of the following:

- The number of messages set by the user.
- The queue's own threshold.
- The percentage of the queue's maximum depth represented by the number of messages in the queue (the "percentage high").

This script is designed to monitor static implementations of WebSphere MQ in which local queues remain fixed. For the monitoring of dynamic implementations of WebSphere MQ, use DynamicLocalQueueDepth (which specifies queue names), because that script does not raise events for queues that were discovered by AppManager but have already been deleted.

Resource Object

MQSeries queue.

Default Schedule

The default interval is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n. If set to **y**, the script returns the number of messages in the local queue.
Use queue's own threshold?	Set to **y** to use the queue threshold defined in the queue's local attributes. An event is raised if the threshold is met or exceeded. The default is n.
Local queue message depth threshold	Enter a threshold for the number of messages in a local queue. An event is raised if the threshold is met or exceeded. The default is 5.
Local queue percentage high threshold	Enter a threshold percentage of the queue's maximum depth represented by the number of messages in the queue. The default is 90%.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

PingQueueManager

Use this Knowledge Script to ping a local queue manager. If the queue manager or the command server is detected down, an event is raised and the Knowledge Script attempts to restart the command server or queue manager.

Resource Object

MQSeries queue manager.

Default Schedule

The default interval is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n. If set to **y**, the script returns a value of 100 if the queue manager is up, or a value of 0 if it is down.
Restart queue manager if down?	Set to **y** to automatically restart the queue manager if it is detected down. The command server will also automatically be restarted if this option is set to **y**. The default is y.
Event Severity if queue manager or command server...	Set the event severity level, from 1 to 40, to reflect the importance when the queue manager or command server: ... **failed to restart or is down**. Severity 5 (red event indicator) ... **restarted successfully**. Severity 12 (yellow event indicator)

ServerDown

Use this Knowledge Script to monitor processes that belong to a specified WebSphere MQ Server user group. An event is raised if there are no processes that belong to the specified WebSphere MQ Server user group.

Resource Object

WebSphereMQUNIX Server.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if over the threshold?	Set to **y** to raise an event if the server is down or the number of processes that belong to the specified user group is 0. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to **y**, this script returns the number of processes belonging to the specified user group running on the server. The default is n.
WebSphere MQ Server user group	Enter the name of the WebSphere MQ Server user group. The default is `mqm`.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

TestQueueManager

Use this Knowledge Script to monitor the connection between the WebSphere MQ Server and a local queue manager. If the WebSphere MQ Server fails to connect to the local queue manager, an event is raised.

This Knowledge Script only establishes that there is a connection between a queue manager and the WebSphere MQ Server. It does not monitor the status of the command server or send any messages to queues. If you need to monitor the command server, or restart either the command server or the local queue manager, use the PingQueueManager Knowledge Script instead.

Resource Object

MQSeries queue manager.

Default Schedule

The default interval is **Every 10 seconds**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the connection between a local queue manager and the WebSphere MQ Server fails. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is n. If set to **y**, the script returns a value of 100 if the queue manager connection is up, or a value of 0 if it is down.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

WebSphereMQErrorLog

Use this Knowledge Script to monitor the WebSphere MQ error log file for specific strings and messages logged since the last monitoring interval. This Knowledge Script allows you to specify the filename and a regular expression to identify the string to look for or to exclude. It then scans the ASCII file and reports the matching entries found since the last monitoring period. It checks for changes to the text file that match the expression you enter; it does not re-scan the entire file at each interval.

In the first interval, this Knowledge Script reads the file and inserts a marker at the end of the file. In subsequent intervals, the script checks the file for changes that match the search criteria you specified. If the file is recreated between intervals and the file size is smaller than the previous version of the file, the script treats the file as a new file and searches the entire file from the beginning. The script raises an event if the number of lines matching your search criteria exceeds the threshold you set.

Use Perl regular expressions to specify the include and exclude patterns.

Resource Object

WebSphereMQUNIX Server.

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n. If set to **y**, the script returns the number of lines containing matching strings.
WebSphere MQ error log file (full path)	Enter the full path to the WebSphere MQ error log file. The default is `/var/mqm/errors/AMQERR01.LOG` You can only specify one file name for any job instance. To monitor multiple logs or files, create separate Knowledge Script jobs.
Regular expression specifying the include filter	Type a regular expression, in Perl, to identify the pattern you want to look for in the text file being monitored. Strings matching the include filter pattern are returned. The default expression matches all strings. For information about writing Perl regular expressions, see “Creating filters with regular expressions” below.
Modifier for the regular expression include filter	Optional modifiers can be used to change the behavior of the regular expression. For example, specifying "i" for this parameter makes the include filter case-insensitive.
Regular expression specifying the exclude filter	Type a regular expression, in Perl, to identify the pattern you want to exclude from matching in the text file being monitored. Strings matching the include filter pattern are returned. For information about writing Perl regular expressions, see “Creating filters with regular expressions” below.

Description	How to Set It
Modifier for the regular expression exclude filter	Optional modifiers can be used to change the behavior of the regular expression. For example, specifying "i" for this parameter makes the exclude filter case-insensitive.
Threshold for matching lines	Enter the number of times to detect a match before raising an event. The default is 0 (the first instance exceeds the threshold and raises an event).
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator). If necessary, adjust the severity, depending on which log or type of event you want.

Creating Filters with Regular Expressions

Some Knowledge Scripts enable you to use regular expressions to define include and exclude filters for pattern-matching against the text being evaluated. Depending on the Knowledge Script you are working with, you may be able to use regular expression include and exclude filters when you are setting job properties, or you may be able to maintain your search criteria independently of the Knowledge Script parameters in a separate filter file. You may also be able to use regular expression modifiers to further refine your filtering.

For example, if your **include filter** looks like this `replic.*` and you specify the modifier `i` to make the search case-insensitive, the regular expression contains the wildcard (`.`) and repeat (`*`) special characters, indicating you want to find strings that start with `replic` followed by any string of characters. Messages containing either `replication` or `replicated` are captured.

The format is the same for the exclude filter. For example, to find log entries that do not start with the string `success`, the exclude filter might look like this:

```
^success.*
```

If you are only searching for included strings, you can leave the exclude filter blank. If you want to retrieve all messages in the log in a given interval, you can specify `.*` for the include filter and leave the exclude filter blank.

Using Special Characters

The following special characters can be used in regular expressions:

Character	Description
.	Wildcard for any one character
*	Repeat zero or more occurrences
^	Beginning of the line
\$	End of the line
\	Escape the next meta-character
|	Alternate matches
[ ]	Any character in the class set. You can specify individual characters or ranges
( )	Grouping characters. For example, you can specify (a|b|c) to indicate a match with a, or b, or c.
+	Quantifier indicating one or more occurrences

Character	Description
?	Quantifier indicating zero or one occurrence
{*n*}	Quantifier indicating exactly *n* occurrence
\w	A word character (alphanumeric plus _)
\s	A white-space character
\d	A digit character

Using Regular Expression Modifiers

In addition to the special characters you can use in creating the regular expression, there are a number of modifiers that can be used to modify how pattern-matching is handled. Valid modifiers include:

Modifier	Description
`c`	Complements the search list
`g`	Matches globally as many times as possible
`i`	Makes the search case-insensitive
`m`	Treats the string as multiple lines
`o`	Interpolates variables only once
`s`	Treats the regular expression string as a single long line
`x`	Allows for regular expression extensions

For additional information about writing regular expressions, see your Perl documentation or other regular expression resources.

Chapter 75
WIN2000 Knowledge Scripts

The Windows 2000 Server (WIN2000) category provides Knowledge Scripts for monitoring Windows servers.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ADDNSRegistrationEventLog	Scans the Event Log for Active Directory-related DNS registration problems.
DFSLinkDown	Monitors the up and down status of a DFS root, link, or replica.
DFSServiceDown	Monitors the up and down status of the DFS service.
DiskQuotaStatus	Monitors disk quota status for the specified logical drive.
DNSAXFRStat	Monitors changes to AXFR statistics for a DNS since the last interval.
DNSDatabaseNodeMemory	Monitors the total memory used by a DNS service for database nodes.
DNSDynaUpdateError	Monitors the number of dynamic update rejections and timeouts during the monitoring interval.
DNSDynaUpdateStat	Monitors the total number of dynamic updates queued by the DNS server.
DNSEventLog	Scans the Windows event log for DNS entries matching your selection criteria.
DNSRecursiveQuery	Monitors recursive queries for the DNS server and checks the number of recursive query errors or timeouts per second.
DNSSecureUpdate	Monitors secure updates for the DNS server and checks the percentage of attempted updates that failed.
DNSTotalQuery	Monitors total query activity for a DNS server and checks the number of queries received per second and the number of responses sent per second.
DNSWINSStat	Monitors the WINS activity for a DNS server.
DNSZoneTransfer	Monitors DNS zone transfer activity and zone transfer failures.
FrsBusy	Monitors the CPU utilization and various statistics of FRS.
FrsEventLog	Scans the Windows FRS log for file replication events.
FrsReplicaError	Monitors the various error statistics of the FRS, including errors in authentication, bindings, and packets sent.
FrsServiceDown	Monitors the up and down status of the FRS.
GroupPolicyAddRemove	Determines whether a Group Policy has been added to or removed from a computer.

Knowledge Script	What It Does
GroupPolicyCount	Counts the number of Group Policies for the target server.
GroupPolicyLinkSnapshot	Lists the links associated with a group policy object.
GroupPolicyRefresh	Refreshes the computer or user group policy on the target server on demand.
GroupPolicySnapshot	Lists all the group policies on the target server.
IASServiceDown	Monitors the up and down status of the Internet Authentication Service.
LSASSWatch	Checks whether the Kerberos Key Distribution Center service process, LSASS, is running or hung.
MSIPackagesChange	Monitors the programs and components installed or uninstalled using the Microsoft Windows Installer (MSI).
PrinterErrors	Monitors printers for problems with printing jobs.
PrinterEventLog	Scans the Windows System log for printer-related events.
PrinterQueue	Monitors the printer queue length.
PrinterUtil	Monitors the bytes per second being handled by the printer.
RemoteStorageEventLog	Scans the Windows Application log for Remote Storage-related events.
RemoteStorageServiceDown	Monitors the up and down status of Remote Storage services.
RSVPEventLog	Scans the Windows Application log for QoS/RSVP-related events.
RSVPServiceDown	Monitors the up and down status of the QoS/RSVP service.
SMTPEventLog	Scans the Windows System log for SMTP-related events.
SMTPQueues	Monitors the queue length for the SMTP queues.
SMTPServiceDown	Monitors the up and down status of the SMTPservice.

ADDNSRegistrationEventLog

Use this Knowledge Script to scan the Event Log for Active Directory-related DNS registration problems. Each time this script runs, it checks the Event Log for entries matching your selection criteria and raises an event if matching entries are found.

Resource Object

DNS folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if log entries match your selection criteria. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information based on the other parameter values you enabled. The default is n.
Start with events in past N hours	Set this parameter to determine which events are searched for the *first* time the Knowledge Script is run. Subsequent searches begin where the last search finished. The following entries are valid: • Enter **-1** to search all current and previous System Log events during the first interval. • Enter **0** to search only for current events; previous events are not searched. • Enter the number of hours to go back in the System Log to scan for matching events. For example, enter 8 to scan the last 8 hours of the System Log for matching entries. The default is 0.
Monitor for events of type:	Set to **y** for each type of event you want to monitor: • Error • Warning • Information • Success Audit • Failure Audit If you enable data collection or events, and set any of these parameters to n, this script does not raise an event or collect data for that type of log entry. The default is y.

Parameter	How to Set It
Filter the [...] field for	To limit the types of entries that raise AppManager for Microsoft Windows events and the type of data that is collected, enter a search string that filters the following fields in the Windows Event Log: • **Category**. Specify one or more text strings to look for in the Category field. Separate multiple strings with commas. • **User**. Specify a search string to look for events associated with a particular user, for example, `<domain name>\<user name>`. Separate multiple strings with commas. For example: `USA\Tom,USA\Chris,EUROPE\Alex`. • **Computer**. Specify computer names to look for. Separate multiple entries with commas. For example: SHASTA,MARS. • **Description**. Specify a detail description or keywords in the description. A string can contain spaces, underscores, and periods. Separate multiple entries with commas. For example: `no domain,critical error from the Active Directory`. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Max number of events per entry	Specify the maximum number of DNS Registration Event Log events that can be returned in each event report. For example, if this value is set to 30, and 67 Registration Event Log events are found, then three event reports are raised: two reports containing 30 events and one report containing seven events. The Message column on the Events tab displays the number of events in the event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration. The default is 30.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the an event in which log entries match your selection criteria. You can adjust the severity based on the types of events you are checking. The default severity level is 8 (red event indicator).

DFSLinkDown

Use this Knowledge Script to monitor Distributed File System (DFS) roots, links, and replicas. For each root replica and link replica, you can check whether the directory for the corresponding replica exists. This script raises an event if any root, root replica, link, or link replica is down.

By default, this script checks the DFS roots and links found during discovery. You can, however, set this script to discover DFS links dynamically each time it runs.

Resource Objects

DFS folder

DFS Root folder

DFS Link object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event Notification	
Create event if root, link, or replica is down?	Set to **Yes** to raise an event when a DFS root, link, or replica is down. The default is Yes.
Severity - DFS volume down	Set the severity level, from 1 to 40, to indicate the importance of an event in which DFS volume is down. The default is 5 (red event indicator).
Severity - DFS path not found	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DFS path cannot be found. The default is 22 (blue event indicator).
Severity - DFS root down	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DFS root is down. The default is 5 (red event indicator).
Severity - DFS root replica down	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DFS root replica is down. The default is 6 (red event indicator).
Severity - DFS link down	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DFS link is down. The default is 7 (red event indicator).
Severity - DFS link replica down	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DFS link replica is down. The default is 8 (red event indicator).
Severity - Job failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DFSLinkDown job fails unexpectedly. The default is 5 (red event indicator).
Data Collection	
Collect data?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns: • **100** -- a root, link, or replica is up, or • **0** -- a root, link, or replica is down. The default is unselected.
Monitoring	

Parameter	How to Set It
Dynamically enumerate DFS root/links?	Set to **Yes** to dynamically enumerate DFS links at each monitoring interval. The default is unselected. **Note** If you select Yes, run this script on the DFS folder object.
Check if the replica directory exists	Set to **Yes** to check for replica directories for each root or link found. The default is unselected. **Note** If the AppManager agent services, NetIQ AppManager Client Resource Monitor (`NetIQmc.exe`) and NetIQ AppManager Client Communication Manager (`NetIQccm.exe`), are running under the Local System account or under a user account that does not have permission to read some directories, checking for replica directories may fail and cause this script to return an error.

DFSServiceDown

Use this Knowledge Script to monitor the up and down status of Distributed File System (DFS) roots, links, and replicas. You can set this script to automatically attempt to restart roots, links, and replicas when they are not running. This script raises an event when auto-start fails, succeeds, or when roots, links, or replicas are down but the *Auto-start service?* parameter is set to n.

Resource Objects

DFS Namespace Service object

DFS Replication Service object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if auto-start fails, succeeds, or is disabled. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the Distributed File System service is up, or • **0** -- the service is down. These values are used to report the percentage of time the service is up in any given period. The default is n.
Auto-start service?	Set to **y** to automatically restart the DFS service when it is down. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager for Microsoft Windows cannot restart it. The default is 5 (red event indicator).
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service was down and AppManager for Microsoft Windows successfully restarted it. The default is 25 (blue event indicator).
Event severity when auto-start is set to n	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and the *Auto-start service?* parameter has been disabled. The default is 18 (yellow event indicator).
Severity for an unexpected KS error	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DFSServiceDown job fails unexpectedly. The default is 35 (magenta event indicator).

DiskQuotaStatus

Use this Knowledge Script to monitor disk quota status. You can set disk quotas to limit the amount of file server disk space for each user. And you can determine how much disk space can be used before a warning is generated. This value is called the warning level.

For example, if the quota limit is set to 10 MB and the warning level is set to 8 MB, a warning message is generated when a user consumes 8 or more megabytes on the file server. When the user reaches the 10 MB quota limit, the user may or may not be able to save any more files, depending on how disk quotas are configured.

This script raises an event if the specified number or percentage of users reaches the warning level or quota limit.

Resource Objects

Disk Quota settings

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event when a threshold is exceeded. The default is y.
Collect data—number of users over quota limit?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of users over the quota limit. The default is n.
Collect data—number of users over warning level?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of users over the warning level. The default is n.
Collect data—number of users below warning level?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of users under the warning level. The default is n.
Collect data—percentage of users over quota limit?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the percentage of users over the quota limit. The default is n.
Collect data—percentage of users over warning level?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the percentage of users over the warning level. The default is n.
Collect data—percentage of users below warning level?	Set to **y t**o collect data for charts and reports. If enabled, data collection returns the percentage of users below the warning level. The default is n.
Collect data—disk space used for each user? (WARNING—heavy load)	Set to **y** to collect data for charts and reports. If enabled, data collection returns the amount of space being used by each user. The default is n. **Note** Large amounts of CPU resources are required for this parameter to return results.
Number of users over limit	Specify the maximum number of users who can be over the quota limit before an event is raised. The default is 1 user.
Number of users over warning level	Specify the maximum number of users who can be over the warning level before an event is raised. The default is 5 users.
Percentage of users over quota limit	Specify the maximum percentage of users who can be over the quota limit before an event is raised. The default is 10%.

Parameter	How to Set It
Percentage of users over warning level	Specify the maximum percentage of users who can be over the warning level before an event is raised. The default is 20%.
Event severity - number of users over quota limit	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of users exceeded the quota threshold. The default is 8 (red event indicator).
Event severity - number of users over warning level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of users exceeds the warning threshold. The default is 15 (yellow event indicator).
Event severity - percentage of users over quota limit	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of users exceeds the quota threshold. The default is 8 (red event indicator).
Event severity - percentage of users over warning level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of users exceeds the warning threshold. The default is 15 (yellow event indicator).
Event severity - API error	Set the event severity level, from 1 to 40, to indicate the importance of an event in which network system errors occur. These errors can be hardware, software, or network related. The default is 7 (red event indicator).

DNSAXFRStat

Use this Knowledge Script to monitor the following AXFR (*zone transfer*, a database replication mechanism) statistics for Master and Secondary Domain Name System (DNS) servers:

- AXFR Request Received (Master)
- AXFR Success Sent (Master)
- AXFR Request Sent (Secondary)
- AXFR Response Received (Secondary)
- AXFR Success Received (Secondary)

This script monitors changes to these statistics since the last interval (delta value), and raises an event if a monitored value exceeds the threshold you set. If you collect data with this script, the AXFR statistics are returned as separate data streams.

Resource Object

DNS folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the number of transfer requests exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the transfer requests sent and received. The default is n.
Transfer requests	Specify the maximum number of transfer requests allowed before an event is raised. The default is 100.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of transfer requests exceeds the threshold. The default is 8 (red event indicator).

DNSDatabaseNodeMemory

Use this Knowledge Script to monitor the total memory used by the Domain Name Service (DNS) service for database nodes. This script raises an event if the memory used by DNS database nodes (in KB) exceeds the threshold you set.

Resource Object

DNS folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the amount of memory used by the DNS service exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the size of database node memory. The default is n.
Memory used (KB)	Specify the maximum amount of memory that can be used by DNS database nodes before an event is raised. The default is 800 KB.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of memory used by the DNS service exceeds the threshold. The default is 8 (red event indicator).

DNSDynaUpdateError

Use this Knowledge Script to monitor the number of Domain Name Service (DNS) dynamic update errors. This script checks for two types of errors:

- Dynamic updates rejected by the DNS server
- Dynamic update timeouts of the DNS server

This script raises an event if the number of dynamic update errors in the interval exceeds the threshold you set.

The dynamic update mechanism allows clients and servers to register DNS domain names and IP address mappings to a DNS server.

Resource Object

DNS folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the number of dynamic update errors exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of dynamic updates rejected and the number of dynamic update timeouts in the interval. The default is n.
Threshold for dynamic update errors	Specify the maximum number of dynamic update errors that can occur in an interval before an event is raised. The default is 2.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of dynamic update errors exceeds the threshold. The default is 8 (red event indicator).

DNSDynaUpdateStat

Use this Knowledge Script to monitor DNS server dynamic update activity. This script raises an event if the dynamic update queue length exceeds the threshold you set. A long queue usually indicates that the DNS server is overloaded and cannot process the update in a timely manner.

The dynamic update mechanism allows clients and servers to register DNS domain names and IP address mappings to a DNS server.

Resource Object

DNS folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the number of dynamic updates in the queue exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the queue length for dynamic updates. To further control the data returned, specify the data collection mode to use. By default, data is not collected.
Data collection mode to use	Specify the type of data you want to collect. The following entries are valid: • **1** - to generate one data stream that records the update queue length. The data detail message describes the number updates received and written per second. • **2** - to generate one data stream that records the update queue length, but without the detail message. • **3** - to generate one data stream that tracks the update queue length, and three additional data streams for the No Operation rate, the rate at which updates are being received, and the rate at which updates are being written to the database. The default is 1 (one data stream and detail message).
Dynamic update queue length	Specify the maximum number of dynamic updates that can be in the queue in an interval before an event is raised. The default is 5 updates.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event if the number of dynamic updates in the queue exceeds the threshold. The default is 8 (red event indicator).

DNSEventLog

Use this Knowledge Script to periodically scan the Domain Name Service (DNS) Server log for DNS events matching the criteria you specify.

In the first interval, the value you specify for the *Start with events in past N hours* parameter determines how far back in the log to check for matching entries. As the script continues to run at subsequent intervals, it checks for any new entries created since the last time the log was checked.

You can further restrict the types of log entries that generate an event in two ways:

- Use the *Monitor for events of type [...]* parameters to search only certain types of events, such as Warning events.
- Use the *Filter the [...] field for* parameters to search only for specific information, such as events associated with a specific user or computer name.

Each time this script runs, it checks the DNS Server log for entries matching your selection criteria and raises an event if matching entries are found. The event detail message returns the text of the log entries found. When this Knowledge Script is set to collect data, it returns the number of log entries found, and the data point detail message returns the text of the log entries.

Resource Object

DNS folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if log entries match your search criteria. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of new event log entries. The graph data detail message contains the text of the log entries. The default is n.
Start with events in past N hours	Set this parameter to determine which events are searched for the *first* time the script is run. Subsequent searches begin where the last search finished. The following entries are valid: • Enter **-1** to search all current and previous DNS Log events during the first interval. • Enter **0** to search only for current events; previous events are not searched. • Enter the number of hours to go back in the DNS Log to scan for matching events. For example, enter 8 to scan the last 8 hours of the DNS Log for matching entries. The default is 0.

Parameter	How to Set It
Monitor for events of type:	Set to **y** for each type of event you want to monitor: • Error • Warning • Information • Success Audit • Failure Audit If you enable data collection or events, and set any of these parameters to n, this script does not raise an event or collect data for that type of log entry. The default is y.
Filter the [...] field for	To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log: • **Source**. Specify one or more text strings to look for in the Source field. Separate multiple strings with commas. For example: `DNS Server,general`. • **Category**. Specify one or more text strings to look for in the Category field. Separate multiple strings with commas. • **Event ID**. Specify a single event ID or a range of event IDs. Separate multiple entries by commas. For example: `414,1028-1400,4015`. • **User**. Specify a search string to look for events associated with a particular user, for example, `<domain name>\<user name>`. Separate multiple strings with commas. For example: `USA\Tom,USA\Chris,EUROPE\Alex`. • **Computer**. Specify a single or multiple computer names to look for. Separate multiple entries by commas. For example: `SHASTA,MARS`. • **Event Description**. Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods. Separate multiple entries with commas. For example: `no domain,critical error from the Active Directory` The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:).
Maximum number of entries per event message	Specify the maximum number of entries to be recorded in each event's detail message. If, during any interval when it scans the log, this script finds more entries in the log than can be put into a single event message, it raises multiple events to return all the log entries. The default is 30 entries.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which log entries match your search criteria. You can adjust the severity level based on the types of events you are checking. The default is 8 (red event indicator).

DNSRecursiveQuery

Use this Knowledge Script to monitor Domain Name Service (DNS) server recursive query activity. This script checks the number of recursive query errors or timeouts per second, and raises an event if the number of recursive query error or timeouts per second exceeds the rate threshold you set.

Resource Object

DNS folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the number of recursive query errors or timeouts exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of recursive queries, failures, and timeouts per second. The default is n.
Recursive query errors/ timeouts	Specify the maximum number of recursive query errors or timeouts per second that can occur before an event is raised. The default is 2.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of recursive query errors or timeouts exceeds the threshold. The default is 8 (red event indicator).

DNSSecureUpdate

Use this Knowledge Script to monitor secure updates for the Domain Name Service (DNS) server, and check the percentage of update attempts that failed. This script raises an event if the percentage of secure update failures exceeds the threshold you set.

Resource Object

DNS folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event in which the percentage of secure updates exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, returns the following information in separate data streams: • Secure update failure rate • Secure update failure number • Secure update total number • Secure update received per second The default is n.
Secure update failures	Specify the maximum percentage of secure updates that are allowed to fail before raising an event. The default is 2%.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percentage of secure updates exceeds the threshold. The default is 8 (red event indicator).

DNSTotalQuery

Use this Knowledge Script to monitor total query activity for a Domain Name Server (DNS) server. This script checks the number of queries received per second and the number of responses sent per second, and raises an event if the query-received rate or the response-sent rate exceeds the threshold you set.

Resource Object

DNS folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the number of query transactions exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of queries received per second and the total number of responses sent per second. The default is n.
Queries received/sent per second	Specify the maximum number of queries that can be received or responses that can be sent per second before an event is raised. The default is 10.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of query transactions exceeds the threshold. The default is 15 (yellow event indicator).

DNSWINSStat

Use this Knowledge Script to monitor the Windows Internet Name Service (WINS) activity for a Domain Name Service (DNS) server. This script checks the number of lookup requests received per second and the number of responses sent per second. This script raises an event if the lookup-received rate, reverse lookup-received rate, response-sent rate, or reverse response-sent rate exceeds the threshold you set.

Resource Object

DNS folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the sent or received rates exceed the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns four data streams: • WINS lookups received per second • WINS responses sent per second • WINS reverse lookups received per second • WINS reverse responses sent per second The default is n.
Lookups received/sent per second	Specify the maximum number of lookups that can be received or responses that can be sent per second before an event is raised. The default is 20 per second.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15 (yellow event indicator).

DNSZoneTransfer

Use this Knowledge Script to monitor Domain Name Service (DNS) zone transfer activity. You can set a threshold for the number of zone transfer failures in an interval and a threshold for the percentage of zone transfers attempted that fail in an interval. This script raises an event if either the number or the percentage of zone transfer failures exceeds the threshold.

Resource Object

DNS folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the number or percentage of zone transfer failures exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns in five separate data streams: • Number of zone transfer failures • Number of successful zone transfers • Number of requests received • Number of SOA (Start of Authority) requests sent • Percentage of zone transfers that failed The default is n.
Zone transfer failures	Specify the maximum number of zone transfer failures that can occur before an event is raised. The default is 5.
Percentage of zone transfer failures	Specify the maximum percentage of zone transfer that can fail before an event is raised. The default is 20%.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number or percentage of zone transfer failures exceeds the threshold. The default severity level is 8 (red event indicator).

FrsBusy

Use this Knowledge Script to monitor the CPU utilization and various statistics of the File Replication Service (FRS). This script raises an event if a threshold is exceeded.

Resource Object

File Replication Service folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, returns data based on the threshold values you set. The default is n.
CPU utilization of the File Replication Service	Specify the maximum percentage of CPU resources the FRS can utilize before an event is raised. The default is 5%.
Number of change orders received	Specify the maximum number of change orders that can be received before an event is raised. The default is 5.
Number of change orders sent	Specify the maximum number of change orders that can be sent before an event is raised. The default is 5.
Number of files installed	Specify the maximum number of replicated files that can be installed locally before an event is raised. The default is 2.
KB of free staging space	Specify the minimum amount of free space in the staging directory that must be available to prevent an event from being raised. The default is 10 KB.
Percentage of free staging space	Specify the minimum percentage of free space in the staging directory that must be available to prevent an event from being raised. The default is 10%.
Number of packets received	Specify the maximum number of packets that can be received before an event is raised. The default is 10.
Number of packets sent	Specify the maximum number of packets that can be sent before an event is raised. The default is 10.
Number of USN records accepted	Specify the maximum number of USN records that can be accepted for replication before an event is raised. The default is 5.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored value exceeds or falls below the threshold. The default is 8 (red event indicator).
Severity for unexpected KS error	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the FrsBusy job fails unexpectedly. The default is 35 (magenta event indicator).

FrsEventLog

Use this Knowledge Script to periodically scan the Windows File Replication Service (FRS) log for file replication events matching the criteria you specify.

Each time this script runs, it checks the FRS log for entries matching the criteria you specify and raises an event if matching entries are found. The event detail message returns the text of the log entries found. When this script is set to collect data, it returns the number of log entries found, and the data point detail message returns the text of the log entries.

In the first interval, the value you specify for the *Start with events in past N hours* parameter determines how far back in the log to check for matching entries. As the script continues to run at subsequent intervals, it checks for any new entries created since the last time the log was checked.

You can further restrict the types of log entries that generate an event in two ways:

- Use the *Monitor for events of type [...]* parameters to search only certain types of events, such as Warning events.
- Use the *Filter the [...] field for* parameters to search only for specific information, such as events associated with a specific user or computer name.

Resource Object

File Replication Service folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if FRS log entries match your search criteria. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of new FRS log entries. The default is n.
Start with events in past N hours	Set this parameter to determine which events are searched for the *first* time this script is run. Subsequent searches begin where the last search finished. The following entries are valid: • Enter **-1** to search all current and previous File Replication Log events during the first interval. • Enter **0** to search only for current events; previous events are not searched. • Enter the number of hours to go back in the FRS Log to scan for matching events. For example, enter 8 to scan the last 8 hours of the File Replication Log for matching entries. The default is 0.

Parameter	How to Set It
Monitor for events of type:	Set to **y** for each type of event you want to monitor: • Error • Warning • Information • Success Audit • Failure Audit If you enable data collection or events, and set any of these parameters to n, this script does not raise an event or collect data for that type of log entry. The default is y.
Filter the [...] field for	To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log: • **Source**. Specify text strings to look for in the Source field. Separate multiple strings with commas. • **Category**. Specify text strings to look for in the Category field. Separate multiple strings with commas. • **Event ID**. Specify a single event ID or a range of event IDs. Separate multiple entries with commas. For example: 414,1028-1400,4015. • **User**. Specify a search string to look for events associated with a particular use, for example, `<domain name>\<user name>`. Separate multiple strings with commas. For example: `USA\Tom,USA\Chris,EUROPE\Alex`. • **Computer**. Specify computer names to look for. Separate multiple entries by commas. For example: SHASTA,MARS. • **Event Description**. Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods. Separate multiple entries with commas. For example: `no domain,critical error from the Active Directory`. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Maximum number of entries per event message	Specify the maximum number of entries to be recorded in each event's detail message. If, during any interval when it scans the log, this script finds more entries in the log than can be put into a single event message, it raises multiple events to return all the log entries. The default is 30 entries.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which FRS log entries match your search criteria. You can adjust the severity level based on the types of events you are checking for. The default is 8 (red event indicator).

FrsReplicaError

Use this Knowledge Script to monitor the various error statistics of the File Replication Service (FRS), including errors in authentication, bindings, and packets sent. This script monitors two objects within the FRS:

- The `FileRelicaConn` object monitors performance statistics for the `Replicaconn` object, which defines replica connections for the DFS roots.
- The `FileReplicaSet` object monitors performance statistics for the `Replicaset` object, which defines a replica set.

This script raises an event if a monitored value exceeds the threshold you set.

Resource Object

File Replication Service folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns data based on the thresholds you set. The default is n.
The number of FileReplicaConn...	Specify the maximum number of errors that can be encountered by the `FileReplicaConn` object before an event is raised in each of these categories: ...authentications in error ...bindings in error ...packets sent in error
The number of FileReplicaSet...	Specify the maximum number of errors that can be encountered by the `FileReplicaSet` object before an event is raised in each of these categories: ...authentications in error ...bindings in error ...DS bindings in error ...DS objects in error ...DS searches in error ...files installed with errors ...packets received in error ...packets sent in error ...staging files generated with errors
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default severity level is 8 (red event indicator).

FrsServiceDown

Use this Knowledge Script to monitor the up and down status of the File Replication Service (FRS). You can set this script to automatically attempt to restart the service when it is not running. This script raises an event when auto-start fails or succeeds, or when the service is down but the *Auto-start service?* parameter is set to n.

Resource Object

File Replication Service object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event when auto-start fails, succeeds, or when the service is down but the *Auto-start service?* parameter is disabled. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the FRS is up • **0** -- the FRS is down These values are used to report the percentage of time the service is up in any given period. The default is n.
Auto-start service?	Set to **y** to automatically restart FRS when it is down. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager for Microsoft Windows cannot restart it. The default is 5 (red event indicator).
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service was down and AppManager for Microsoft Windows successfully restarted it. The default is 25 (blue event indicator).
Event severity when auto-start is set to n	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and the *Auto-start service?* parameter has been disabled. The default is 18 (yellow event indicator).
Severity for an unexpected KS error	Set the level between 1 and 40, to indicate the importance of an event in which the FrsServiceDown job fails unexpectedly. The default is 35 (magenta event indicator).

GroupPolicyAddRemove

Use this Knowledge Script to check whether a Group Policy has been added to or removed from a target computer. This script raises an event if a Group Policy is added or removed during the monitoring interval.

Resource Object

Group Policy top-level folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if a Group Policy is added or removed during the monitoring interval. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- there were no Group Policy changes, or • **0** -- a Group Policy was added or removed during the interval. The default is n.
Event severity when a Group Policy is added	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a Group Policy was added during the monitoring period. The default is 5 (red event indicator).
Event severity when a Group Policy is removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a Group Policy was removed during the monitoring period. The default is 5 (red event indicator).

GroupPolicyCount

Use this Knowledge Script to count the number of Group Policies associated with the target server in Active Directory. This script raises an event if the number of Group Policies associated with the server exceeds the threshold you set.

Resource Object

Group Policy top-level folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the number of Group Policies exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of Group Policies found. The default is n.
Group Policies	Specify the maximum number of Group Policies that can be associated with a computer in Active Directory before an event is raised. The default is 5 Group Policies.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of Group Policies exceeds the threshold. The default is 5 (blue event indicator).

GroupPolicyLinkSnapshot

Use this Knowledge Script to list the links associated with one or multiple Group Policy objects. This script raises an event if Group Policy links are found or not found.

Resource Object

Windows Server 2003 Group Policy object

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if Group Policy links are found or not found. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of Group Policy links found. The default is n.
Event severity when Group Policy link is found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Group Policy links have been detected and returned in the event detail message. The default is 25 (blue event indicator).
Event severity when Group Policy link is not found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no Group Policy links have been detected. The default is 5 (red event indicator).

GroupPolicyRefresh

Use this Knowledge Script to refresh the computer Group Policy or the user Group Policy without restarting the computer or re-entering login information. This script refreshes the computer or user policy for all the Group Policies associated with the target computer.

Resource Object

Group Policy folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event for a successful refresh policy?	Set to **y** to raise an event when the refresh succeeds. This script always raises an event when the refresh fails. The default is y.
Refresh computer group policy?	Set to **y** to refresh the computer Group Policy. The default is y.
Refresh user group policy?	Set to **y** to refresh the user Group Policy. The default is n.
Event severity when a refresh is successful	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a refresh of the computer or user Group Policy succeeds. The default is 25 (blue event indicator).
Event severity when a refresh fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a refresh of the computer or user Group Policy fails. The default is 25 (blue event indicator).

GroupPolicySnapshot

Use this Knowledge Script to list all the Group Policies on the target server in priority order. This script raises an event if Group Policies are found. If you enable data collection, the event detail message lists all the Group Policies sorted in the following priority order:

- Local Group Policies are listed first
- Default Domain Group Policy are listed second
- Default Domain Controller Group Policy are listed last

No event is raised if no Group Policies are found for the target computer.

Resource Object

Group Policy top-level folder

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if Group Policies are found. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of Group Policies found. The default is n.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Group Policies are found. The default is 25 (blue event indicator).

IASServiceDown

Use this Knowledge Script to monitor up and down status of the Internet Authentication Service (IAS). You can set this script to automatically attempt a service restart when it is not running. This script raises an event when auto-start fails, succeeds, or is disabled.

Resource Object

Internet Authentication Service object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if auto-starts fails, succeeds, or is disabled. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the Internet Authentication Service is up, or • **0** -- the service is down. These values are used to report the percentage of time the service is up in any given period. The default is n.
Auto-start service?	Set to **y** to automatically restart IAS when it is down. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager for Microsoft Windows cannot restart it. The default is 5 (red event indicator).
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service was down and AppManager for Microsoft Windows successfully restarted it. The default is 25 (blue event indicator).
Event severity when auto-start is set to n	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and the *Auto-start service?* parameter has been disabled. The default is 18 (yellow event indicator).
Severity for an unexpected KS error	Set the level between 1 and 40, to indicate the importance of an event in which the IASServiceDown job fails unexpectedly. The default is 35 (magenta event indicator).

LSASSWatch

Use this Knowledge Script to check whether the Kerberos Key Distribution Center service (specifically, the LSASS process) is running or hung. This script also monitors the amount of CPU time the LSASS process is using. You specify the threshold for CPU usage and the number of consecutive times the threshold can be exceeded before raising an event.

This script raises an event if the LSASS process is not running or if the process is using a large amount of CPU over a consecutive number of intervals (known as looping).

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if CPU usage exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the process is running, or • **0** -- the process is down. The default is n.
High CPU usage	Specify the maximum amount of CPU that the LSASS process can consume before an event is raised. The default is 90%.
Consecutive times LSASS has high CPU usage	Specify the consecutive number of intervals the CPU usage of the LSASS process can exceed the threshold before an event is raised. The default is 3 times.
Event severity - Process appears to be hung	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the LSASS process is hung, or looping. The default is 5 (yellow event indicator).
Event severity - Process is not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the LSASS process is not running. The default is 15 (yellow event indicator).

MSIPackagesChange

Use this Knowledge Script to monitor the programs or components installed or uninstalled using the Microsoft Windows Installer (MSI). This script tracks the changes recorded in the registry under `SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall` and reports the number of MSI packages that were installed, uninstalled, or updated during the monitoring period.

If you enable detailed data collection, the name, version, publication name, and installation date are returned for each MSI package.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Daily**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if an MSI package is installed, uninstalled, or updated. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of currently installed packages. The default is n.
Create data detail message with package information	Set to **y** to generate the data detail message including package name, version, publication name, and installation date. The default is n.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an MSI package is installed, uninstalled, or updated. The default is 8 (red event indicator).

PrinterErrors

Use this Knowledge Script to monitor printer-related errors:

- Print job errors (such as, print jobs that are hung because of data transfer problems or paper jams)
- Printer not ready errors
- Printer out of paper errors

You can set a separate threshold for each type of printer error. This script raises an event if any error type exceeds the threshold you set.

Note
To run this script successfully, avoid using special characters such as, /, -, and # when defining the printer name on the monitored computers. Also, if you run the Discovery_NT Knowledge Script and then delete a local or network printer, run Discovery_NT again.

Resource Object

Printer object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the process is running, or • **0** -- the process is down. The default is n.
Threshold for the number of "Print job" errors	Specify the maximum number of print job errors that can occur in an interval before an event is raised. The default is 5 errors.
Threshold for the number of "Printer not ready" errors	Specify the maximum number of printer "not ready" errors that can occur in an interval before an event is raised. The default is 5 errors.
Threshold for the number of "Out of paper" errors	Specify the maximum number of "out of paper" errors that can occur in an interval before an event is raised. The default is 10 errors.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8 (red event indicator).

PrinterEventLog

Use this Knowledge Script to periodically scan the Windows System log for printer-related events matching the criteria you specify.

Each time this script runs, it checks the System log for entries matching your selection criteria and raises an event if matching entries are found. The event detail message returns the text of the log entries found. When this script is set to collect data, it returns the number of log entries found, and the data point detail message returns the text of the log entries.

In the first interval, the value you specify for the *Start with events in past N hours* parameter determines how far back in the log to check for matching entries. As the script continues to run at subsequent intervals, it checks for any new entries created since the last time the log was checked.

You can further restrict the types of log entries that generate an event in two ways:

- Use the *Monitor for events of type [...]* parameters to search only certain types of events, such as Warning events.
- Use the *Filter the [...] field for* parameters to search only for specific information, such as events associated with a specific user or computer name.

Note
To run this script successfully, avoid using special characters such as /, -, and # when defining the printer name on the monitored computers. Also, if you run the Discovery_NT Knowledge Script and then delete a local or network printer, you must run Discovery_NT again.

Resource Object

Printer folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if log entries match your search criteria. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of new event log entries. The default is n.
Start with events in past N hours	Set this parameter to determine which events are searched for the *first* time the script is run. Subsequent searches begin where the last search finished. The following entries are valid: • Enter **-1** to search all current and previous System Log events during the first interval. • Enter **0** to search only for current events; previous events are not searched. • Enter the number of hours to go back in the System Log to scan for matching events. For example, enter 8 to scan the last 8 hours of the System Log for matching entries. The default is 0.

Parameter	How to Set It
Monitor for events of type:	Set to **y** for each type of event you want to monitor: • Error • Warning • Information • Success Audit • Failure Audit If you enable data collection or events, and set any of these parameters to n, this script does not raise an event or collect data for that type of log entry. The default is y.
Filter the [...] field for	To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log: • **Category**. Specify text strings to look for in the Category field. Separate multiple strings with commas. • **Event ID**. Specify a single event ID or a range of event IDs. Separate multiple entries by commas. For example: 414,1028-1400,4015. • **User**. Specify a search string to look for events associated with a particular user, for example, `<domain name>\<user name>`. Separate multiple strings with commas. For example: `USA\Tom,USA\Chris,EUROPE\Alex`. • **Computer**. Specify computer names to look for. Separate multiple entries by commas. For example: SHASTA,MARS. • **Event Description**. Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods. Separate multiple entries with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Maximum number of entries per event message	Specify the maximum number of entries to be recorded in each event's detail message. If, during any interval when it scans the log, the script finds more entries in the log than can be put into a single event message, it raises multiple events to return all the log entries. Default is 30 entries.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the log contains entries that match your search criteria. You can adjust the severity based on the types of events you are checking. The default is 8 (red event indicator).

PrinterQueue

Use this Knowledge Script to monitor the printer queue length. This script raises an event if the printer queue length exceeds the threshold you set.

This script is not supported on 64-bit systems.

Note
To run this script successfully, avoid using special characters such as, /, -, and # when defining the printer name on the monitored computers. Also, if you run the Discovery_NT Knowledge Script and then delete a local or network printer, run Discovery_NT again.

Resource Object

Local or cluster printer object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the number of print jobs in the queue exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the current printer queue length. The default is n.
Threshold for printer queue length	Specify the maximum number of print jobs that can be in the printer queue before an event is raised. The default is 5 jobs.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of print jobs in the queue exceeds the threshold. The default is 8 (red event indicator).

PrinterUtil

Use this Knowledge Script to monitor printer utilization by tracking the number of bytes printed per second. This script raises an event if the number of bytes per second exceeds the threshold you set.

Note
To run this script successfully, avoid using special characters such as, /, -, and # when defining the printer name on the monitored computers. Also, if you run the Discovery_NT Knowledge Script and then delete a local or network printer, run Discovery_NT again.

Resource Object

Local or cluster printer object

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the number of bytes printed per second exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of bytes printed per second. The default is n.
Threshold for bytes printed per second	Specify the maximum number of bytes that can be printed per second before an event is raised. The default is 2000 bytes.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of bytes printed per second exceeds the threshold. The default is 8 (red event indicator).

RemoteStorageEventLog

Use this Knowledge Script to periodically scan the Windows Application log for Remote Storage-related events matching the criteria you specify.

Each time this script runs, it checks the Application log for entries matching your selection criteria and raises an event if matching entries are found. The event detail message returns the text of the log entries found. When this script is set to collect data, it returns the number of log entries found, and the data point detail message returns the text of the log entries.

In the first interval, the value you specify for the *Start with events in past N hours* parameter determines how far back in the log to check for matching entries. As the script continues to run at subsequent intervals, it checks for any new entries created since the last time the log was checked.

You can further restrict the types of log entries that generate an event in two ways:

- Use the *Monitor for events of type [...]* parameters to search only certain types of events, such as Warning events.
- Use the *Filter the [...] field for* parameters to search only for specific information, such as events associated with a specific user or computer name.

Resource Object

Remote Storage folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if log entries match your search criteria. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of new event log entries. The default is n.
Start with events in past N hours	Set this parameter to determine which events are searched for the *first* time the script is run. Subsequent searches begin where the last search finished. The following entries are valid: • Enter **-1** to search all current and previous Application Log events during the first interval. • Enter **0** to search only for current events; previous events are not searched. • Enter the number of hours to go back in the Application Log to scan for matching events. For example, enter 8 to scan the last 8 hours of the Application Log for matching entries. The default is 0.

Parameter	How to Set It
Monitor for events of type:	Set to **y** for each type of event you want to monitor: • Error • Warning • Information • Success Audit • Failure Audit If you enable data collection or events, and set any of these parameters to n, this script does not raise an event or collect data for that type of log entry. The default is y.
Filter the [...] field for	To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log: • **Category**. Specify text strings to look for in the Category field. Separate multiple strings with commas. • **Event ID**. Specify a single event ID or a range of event IDs. Separate multiple entries by commas. For example: 414,1028-1400,4015. • **User**. Specify a search string to look for events associated with a particular user, for example, `<domain name>\<user name>`. Separate multiple strings with commas. For example: `USA\Tom,USA\Chris,EUROPE\Alex`. • **Computer**. Specify a single or multiple computer names to look for. Separate multiple entries by commas. For example: SHASTA,MARS. • **Event Description**. Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods. Separate multiple entries with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Maximum number of entries per event message	Specify the maximum number of entries to be recorded in each event's detail message. If, during any interval when it scans the log, this script finds more entries in the log than can be put into a single event message, it raises multiple events to return all the log entries. The default is 30 entries.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which log entries match your search criteria. You can adjust the severity based on the types of events you are checking. The default is 8 (red event indicator).

RemoteStorageServiceDown

Use this Knowledge Script to monitor the up and down status of the Remote Storage Service. You can set this script to automatically attempt to restart the service when it is not running. This script raises an event when auto-start fails, succeeds, or is disabled.

Resource Object

Remote Storage folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if auto-start fails, succeeds, or is disabled. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the Remote Storage services are up, or • **0** -- any service is down. These values are used to report the percentage of time the service is up in any given period. The default is n.
Auto-start service?	Set to **y** to automatically restart any Remote Storage service when it is down. The default is y.
Severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which service is down and AppManager for Microsoft Windows cannot restart it. The default is 5 (red event indicator).
Severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service was down and AppManager for Microsoft Windows successfully restarted it. The default is 25 (blue event indicator).
Severity when auto-start is set to n	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and the *Auto-start service?* parameter has been disabled. The default is 18 (yellow event indicator).
Severity for an unexpected KS error	Set the level between 1 and 40, to indicate the importance of an event in which the RemoteStorageServiceDown job fails unexpectedly. The default is 35 (magenta event indicator).

RSVPEventLog

Use this Knowledge Script to periodically scan the Windows Application log for QoS/RSVP-related events matching the criteria you specify.

Each time this script runs, it checks the Application log for entries matching your selection criteria and raises an event if matching entries are found. The event detail message returns the text of the log entries found. When data collection is enabled, the job returns the number of log entries found, and the data point detail message returns the text of the log entries.

In the first interval, the value you specify for the *Start with events in past N hours* parameter determines how far back in the log to check for matching entries. As the script continues to run at subsequent intervals, it checks for any new entries created since the last time the log was checked.

You can further restrict the types of log entries that generate an event in two ways:

- Use the *Monitor for events of type [...]* parameters to search only certain types of events, such as Warning events.
- Use the *Filter the [...] field for* parameters to search only for specific information, such as events associated with a specific user or computer name.

Resource Object

QoS folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if log entries match your search criteria. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of new event log entries. The graph data detail message returns the text of the log entries. The default is n.
Start with events in past N hours	Set this parameter to determine which events are searched for the *first* time the Knowledge Script is run. Subsequent searches begin where the last search finished. The following entries are valid: • Enter **-1** to search all current and previous Application Log events during the first interval. • Enter **0** to search only for current events; previous events are not searched. • Enter the number of hours to go back in the Application Log to scan for matching events. For example, enter 8 to scan the last 8 hours of the Application Log for matching entries. The default is 0.

Parameter	How to Set It
Monitor for events of type:	Set to **y** for each type of event you want to monitor: • Error • Warning • Information • Success Audit • Failure Audit If you enable data collection or events, and set any of these parameters to n, this script does not raise an event or collect data for that type of log entry. The default is y.
Filter the [...] field for	To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log: • **Category**. Specify text strings to look for in the Category field. Separate multiple strings with commas. • **Event ID**. Specify a single event ID or a range of event IDs. Separate multiple entries by commas. For example: 414,1028-1400,4015. • **User**. Specify a search string to look for events associated with a particular user, for example, `<domain name>\<user name>`. Separate multiple strings with commas. For example: `USA\Tom,USA\Chris,EUROPE\Alex`. • **Computer**. Specify computer names to look for. Separate multiple entries by commas. For example: SHASTA,MARS. • **Event Description**. Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods. Separate multiple entries with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Maximum number of entries per event message	Specify the maximum number of entries to be recorded in each event's detail message. If, during any interval when it scans the log, the script finds more entries in the log than can be put into a single event message, it raises multiple events to return all the log entries. The default is 30 entries.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which log entries match your search criteria. You can adjust the severity based on the types of events you are checking. The default is 8 (red event indicator).

RSVPServiceDown

Use this Knowledge Script to monitor the Windows QoS/RSVP service. You can set this script to automatically attempt to restart the service when it is not running. This script raises an event if the service is not running, if the attempt to restart it fails, or if the service is down and the *Auto-start service?* parameter is set to n.

Resource Object

QoS folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if the service is not running, if the restart attempt fails, or if the service is down and the *Auto-start service?* parameter is set to n. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the QoS/RSVP service is up, or • **0** -- the service is down. These values are used to report the percentage of time the service is up in any given period. The default is n.
Auto-start service?	Set to **y** to automatically restart the QoS/RSVP service when it is down. The default is y.
Severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which service is down and AppManager for Microsoft Windows cannot restart it. The default is 5 (red event indicator).
Severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service was down and AppManager for Microsoft Windows successfully restarted it. The default is 25 (blue event indicator).
Severity when auto-start is set to n	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and the *Auto-start service?* parameter is set to n. The default is 18 (yellow event indicator).
Severity for an unexpected KS error	Set the level between 1 and 40, to indicate the importance of an event in which the RSVPServiceDown job fails unexpectedly. The default is 35 (magenta event indicator).

SMTPEventLog

Use this Knowledge Script to periodically scan the Windows System log for SMTP-related events matching the criteria you specify.

Each time this script runs, it checks the System log for entries matching your selection criteria and raises an event if matching entries are found. The event detail message returns the text of the log entries found. When this script is set to collect data, it returns the number of log entries found, and the data point detail message returns the text of the log entries.

In the first interval, the value you specify for the *Start with events in past N hours* parameter determines how far back in the log to check for matching entries. As the script continues to run at subsequent intervals, it checks for any new entries created since the last time the log was checked.

You can further restrict the types of log entries that generate an event in two ways:

- Use the *Monitor for events of type [...]* parameters to search only certain types of events, such as Warning events.
- Use the *Filter the [...] field for* parameters to search only for specific information, such as events associated with a specific user or computer name.

Resource Object

SMTP folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if log entries match your search criteria. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of new event log entries. The default is n.
Start with events in past N hours	Set this parameter to determine which events are searched for the *first* time this script is run. Subsequent searches begin where the last search finished. The following entries are valid: • Enter **-1** to search all current and previous System Log events during the first interval. • Enter **0** to search only for current events; previous events are not searched. • Enter the number of hours to go back in the System Log to scan for matching events. For example, enter 8 to scan the last 8 hours of the System Log for matching entries. The default is 0.

Parameter	How to Set It
Monitor for events of type:	Set to **y** for each type of event you want to monitor: • Error • Warning • Information • Success Audit • Failure Audit If you enable data collection or events, and set any of these parameters to n, this script does not raise an event or collect data for that type of log entry. The default is y.
Filter the [...] field for	To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log: • **Category**. Specify text strings to look for in the Category field. Separate multiple strings with commas. • **Event ID**. Specify a single event ID or a range of event IDs. Separate multiple entries by commas. For example: `414,1028-1400,4015`. • **User**. Specify a search string to look for events associated with a particular user, for example, `<domain name>\<user name>`. Separate multiple strings with commas. For example: `USA\Tom,USA\Chris,EUROPE\Alex`. • **Computer**. Specify computer names to look for. Separate multiple entries by commas. For example: `SHASTA,MARS`. • **Event Description**. Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods. Separate multiple entries with commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Maximum number of entries per event message	Specify the maximum number of entries to be recorded in each event's detail message. If, during any interval when it scans the log, this script finds more entries in the log than can be put into a single event message, it raises multiple events to return all the log entries. The default is 30 entries.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which log entries match your search criteria. You can adjust the severity based on the types of events you are checking. The default is 8 (red event indicator).

SMTPQueues

Use this Knowledge Script to monitor the length of the following SMTP queues:

- Categorizer queue
- Local queue
- Local Retry queue
- Remote queue
- Remote Retry queue

This script raises an event if any queue length exceeds the threshold you set.

Resource Object

SMTP folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event if a queue length exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the queue length for each SMTP queue. The default is n.
SMTP Categorizer queue length	Specify the maximum number of processes that can be in the SMTP Categorizer queue before an event is raised. The default is 10.
SMTP Local queue length	Specify the maximum number of processes that can be in the SMTP Local queue before an event is raised. The default is 10.
SMTP Local Retry queue length	Specify the maximum number of processes that can be in the SMTP Local Retry queue before an event is raised. The default is 5.
SMTP Remote queue length	Specify the maximum number of processes that can be in the SMTP Remote queue before an event is raised. The default is 10.
SMTP Remote Retry queue length	Specify the maximum number of processes that can be in the SMTP Remote Retry queue before an event is raised. The default is 5.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a queue length exceeds the threshold you set. The default is 8 (red event indicator).

SMTPServiceDown

Use this Knowledge Script to monitor the up and down status of the SMTP service. You can set this script to automatically attempt to restart the service when it is not running. This script raises an event when auto-start fails, succeeds, or is disabled.

Resource Object

SMTP Service object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise an event when auto-start fails, succeeds, or is disabled. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • **100** -- the SMTP service is up, or • **0** -- the service is down. These values are used to report the percentage of time the service is up in any given period. The default is n.
Auto-start service?	Set to **y** to automatically restart the SMTP service when it is down. The default is y.
Severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which service is down and AppManager for Microsoft Windows cannot restart it. The default is 5 (red event indicator).
Severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service was down and AppManager for Microsoft Windows successfully restarted it. The default is 25 (blue event indicator).
Severity when auto-start is set to n	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and the *Auto-start service?* parameter is set to n. The default is 18 (yellow event indicator).
Severity for an unexpected KS error	Set the level between 1 and 40, to indicate the importance of an event in which the SMTPServiceDown job fails unexpectedly. The default is 35 (magenta event indicator).

Chapter 76
WIN2003 Knowledge Scripts

The WIN2003 category provides Knowledge Scripts for monitoring Microsoft Windows Server 2003, Microsoft Windows XP Professional, and Microsoft Windows Server 2008.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
ActivationGracePeriod	Monitors the number of days that remain before you are required to activate the Windows operating system.
AUDownLoaded	Monitors the number of critical Windows updates that have been downloaded but not yet installed
AUOptionChange	Monitors the Automatic Updates options.
AUServiceDown	Monitors the status of the Automatic Updates service
AUVerifyHotFix	Verifies whether specified hotfixes have been installed.
BITSJobProgress	Monitors the progress of Background Intelligent Transfer Service jobs by measuring the total bytes transferred and the total files transferred.
BITSJobsActive	Monitors the number of active Background Intelligent Transfer Service jobs.
BITSJobsError	Monitors the total number of Background Intelligent Transfer Service jobs that are in an error state.
BITSJobState	Indicates whether a Background Intelligent Transfer Service job is in error state or not in error state.
BITSJobStats	Monitors the number of times a Background Intelligent Transfer Service job is interrupted by network failure or server unavailability.
BITSServiceDown	Monitors the status of the Background Intelligent Transfer Service.
CLRConnectionPools	Monitors SQL connection pools in managed .NET applications.
CLRContention	Monitors the thread contention rate and thread queue length in managed .NET applications.
CLRExceptions	Monitors exceptions that managed .NET applications raise.
CLRHeap	Monitors heap memory use in managed .NET applications.
CLRJit	Monitors JIT (just-in-time) compilation in managed .NET applications.
CLRMemProfile	Monitors total garbage collection in managed .NET applications.
CLRNetworking	Monitors network activity in managed .NET applications.
CLRRemoting	Monitors remote procedure call (RPC) activity in managed .NET applications.

Knowledge Script	What It Does
CLRThreads	Monitors thread use in managed .NET applications.
DCOMAppChange	Monitors the distributed COM (DCOM) application list.
FaxActivity	Monitors the number of faxes, fax pages, and fax bytes sent and received.
FaxEventLog	Scans the Windows Application event log for entries created by the Microsoft Fax service that match the criteria you specify.
FaxServiceDown	Monitors the status of the Microsoft Fax service.
FaxTotalFailed	Monitors the total number of failed faxes, failed outgoing connections, and failed receptions.
FaxTotalTime	Monitors the number of minutes the Microsoft Fax service spends receiving and sending faxes.
OpenSystemSlots	Monitors the number of available system (PCI) slots.
PNPDeviceChange	Monitors the plug-and-play device list for any device that has been added or removed since the script was last run.
PNPDeviceErrors	Monitors the number of plug-and-play devices that have a status of “error.”
PrinterStuckJobs	Monitors jobs that are stuck in the printer queue.
SRDiskPercent	Monitors the percentage of space on a disk available for the System Restore service.
SREventLog	Scans the Windows Application event log for entries created by the System Restore service that match the criteria you specify.
SRLifeInterval	Monitors the number of days the System Restore service preserves System Restore points
SRPoints	Monitors the number of System Restore points that are being preserved by the System Restore service.
SRScheduledInterval	Monitors the interval at which scheduled System Restore points are created during both current and global sessions.
SRServiceDown	Monitors the status of the System Restore service.

ActivationGracePeriod

Use this Knowledge Script to monitor the number of days that remain before you are required to activate the system. After you install Windows, you must activate your installation by contacting Microsoft. If you do not activate within a certain number of days, you can no longer log on.

This script raises an event if the number of days remaining falls below the threshold you set.

Resource Objects

32-bit or 64-bit AMD- and Intel-based computers running the following:

- *For AppManager version 7.x*: Windows Server 2003, Windows XP Professional, Windows Server 2008 (including R2), Windows 7
- *For AppManager version 6.x*: Windows Server 2003, Windows XP Professional

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if number of days in grace period falls below threshold?	Set to **y** to raise an event when the number of days remaining before you must activate the system falls below the threshold you set. The default is y.
Collect data for days remaining in grace period?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of days remaining before you must activate your system. The default is n.
Threshold -- Minimum days remaining in grace period	Specify the minimum number of days that must remain before activation of the system is required to prevent an event from being raised. The default is 1 day.
Event severity when number of days falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of days remaining before system activation is required falls below the threshold. The default is 5 (red event indicator).

AUDownLoaded

Use this Knowledge Script to monitor the total number of critical updates from the Windows update Web site that have been downloaded but not yet installed. If you configure Automatic Updates to prompt you before installing downloaded updates, then you may accumulate a large number of downloaded updates that have not yet been installed. This script raises an event if the total number of downloaded, but uninstalled, updates exceeds the threshold you set.

Resource Object

Automatic Updates folder

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the total number of updates downloaded exceeds the threshold you set. The default is y.
Collect data for updates downloaded but not installed?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of updates that have been downloaded but not yet installed. The default is n.
Threshold -- Maximum total downloaded updates	Specify the maximum number of updates that can be downloaded but not installed before an event is raised. The default is 10.
Event severity when downloaded updates exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of updates that can be downloaded but not installed exceeds the threshold. The default is 8 (red event indicator).

AUOptionChange

Use this Knowledge Script to monitor the Automatic Updates options. You can configure several Automatic Updates options:

- Disabled
- Notify user before download and install
- Download automatically and notify before install
- Automatically download and install on schedule

This script raises an event is raised if an option setting is changed.

Resource Object

Automatic Updates folder

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if Automatic Updates option changed?	Set to **y** to raise an event when an option setting is changed. The default is y.
Collect data for Automatic Updates options changed?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the current selections for the Automatic Updates options. The default is n.
Event severity when option changed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which Automatic Updates options have changed. The default is 8 (red event indicator).

AUServiceDown

Use this Knowledge Script to monitor the status of the Automatic Updates service. This script raises an event if the service is down, and can, optionally, attempt to restart the service when it is not running.

Resource Object

Automatic Updates Service object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if Automatic Updates service is down?	Set to **y** to raise an event when the Automatic Updates service is down. The default is y.
Collect data for service status?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • 100 -- service is running, or • 0 -- service is not running. The default is n.
Auto-start service if down?	Set to **y** to automatically restart the service when it is down. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager cannot restart it. The default is 5 (red event indicator).
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service was down and AppManager successfully restarted it. The default is 25 (blue event indicator).
Event severity when service down and auto-start disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager has been set to not restart the service. The default is 18 (yellow event indicator).

AUVerifyHotFix

Use this Knowledge Script to verify whether the hotfixes you specify have been installed. This script raises an event when specified hotfixes have not been installed and when specified hotfixes are installed.

Resource Object

Automatic Updates folder

Default Schedule

The default interval for this script is once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Hotfix articles to monitor	Specify the ID for each hotfix you want to verify. You can enter multiple IDs separated by commas. **Note** The ID for each hotfix is case-sensitive. For example, Q123456 is *not* a match for q123456. If your entry does not exactly match the hotfix ID, an event is raised indicating the hotfix in question has not been installed even if it has been installed.
Raise event when hotfixes are installed?	Set to **y** to raise an event when the hotfixes you specify have been installed. The default is y.
Event severity when hotfixes are installed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which specified hotfixes have been installed. The default is 15 (yellow event indicator).
Raise event if hotfixes have not been installed?	Set to **y** to raise an event when the hotfixes you specify have not yet been installed. The default is y.
Event severity when hotfixes have not been installed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the hotfixes you specified have not been installed. The default is 8 (red event indicator).
Collect data for installed hotfixes?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of installed hotfixes. The default is n.

BITSJobProgress

Use this Knowledge Script to monitor the progress of Background Intelligent Transfer Service (BITS) jobs by measuring the total bytes transferred and the total files transferred. This script raises an event if the total number of bytes or files transferred exceeds the thresholds you set.

Prerequisite

This script runs only on 32-bit platforms and requires version 2.0 or later of Windows .NET Framework to be installed on the computer you want to monitor.

Resource Objects

BITS Jobs object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if the total bytes transferred or the total files transferred exceed the threshold you set. The default is y.
Collect data for total bytes and files transferred by BITS jobs?	Set to **y** to collect data for charts and reports. If enabled, data collection returns total bytes transferred and total files transferred for a BITS job. The default is n.
Threshold -- Maximum number of bytes transferred by BITS jobs	Specify the maximum number of bytes that can be transferred before an event is raised. The default is 200 bytes.
Threshold -- Maximum number of files transferred by BITS jobs	Specify the maximum number of files that can be transferred before an event is raised. The default is 200 files.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of transferred bytes or jobs exceeds the threshold you set. The default is 8 (red event indicator).

BITSJobsActive

Use this Knowledge Script to monitor the number of active BITS jobs. This script raises an event when the total number of active jobs exceeds the threshold.

Prerequisite

This script runs only on 32-bit platforms and requires version 2.0 or later of Windows .NET Framework to be installed on the computer you want to monitor.

Resource Object

BITS folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if number of active BITS jobs exceeds threshold?	Set to **y** to raise an event when the total number of active BITS jobs exceeds the threshold you set. The default is y.
Collect data for number of active BITS jobs?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of jobs submitted and the number of incomplete jobs during the interval you specify. The default is n.
Threshold -- Maximum number of active BITS jobs	Specify the maximum number of BITS jobs that can be active before an event is raised. The default is 200 jobs.
Event severity when number of active BITS jobs exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of active BITS jobs exceeds the threshold. The default is 8 (red event indicator).

BITSJobsError

Use this Knowledge Script to monitor the total number of BITS jobs that are in an error state. This script raises an event if the number of BITS jobs with the status of error exceeds the threshold.

Prerequisite

This script runs only on 32-bit platforms and requires version 2.0 or later of Windows .NET Framework to be installed on the computer you want to monitor.

Resource Object

BITS folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if number of BITS jobs in error state exceeds threshold?	Set to **y** to raise an event when the number of BITS jobs with the status of error exceeds the threshold you set. The default is y.
Collect data for BITS jobs in error state?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of BITS jobs that have the status of error. The default is n.
Threshold -- Maximum number of BITS jobs in error state	Specify the maximum number of BITS jobs that can have a status of error before an event is raised. The default is 10.
Event severity when BITS jobs in error state exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of BITS job with a status of error exceeds the threshold. The default is 8 (red event indicator).

BITSJobState

Use this Knowledge Script to monitor the state of a BITS job. This script raises an event if a BITS job is in error state and when it is not in error state.

Prerequisite

This script runs only on 32-bit platforms and requires version 2.0 or later of Windows .NET Framework to be installed on the computer you want to monitor.

Resource Object

BITS Job object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if BITS job is in error state?	Set to **y** to raise an event when the BITS job is in the error state. The default is y.
Raise event if BITS job is not in error state?	Set to **y** to raise an event when the BITS job is not in the error state. The default is y.
Collect data for status of BITS job?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the state of the BITS job: canceled, executing, completed, or error. The default is n.
Event severity when BITS job in error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BITS job is in an error state. The default is 8 (red event indicator).
Event severity when BITS job not in error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the BITS job is not in an error state. The default is 25 (blue event indicator).

BITSJobStats

Use this Knowledge Script to monitor the number of times the BITS job is interrupted by network failure or server unavailability. This script raises an event is raised if the total number of times the BITS job is interrupted exceeds the threshold.

Prerequisite

This script runs only on 32-bit platforms and requires version 2.0 or later of Windows .NET Framework to be installed on the computer you want to monitor.

Resource Object

BITS Jobs object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if interruptions exceed threshold?	Set to **y** to raise an event when the number of times the BITS job is interrupted exceeds the threshold you set. The default is y.
Collect data for number of BITS job interruptions?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of times the BITS job is interrupted. The default is n.
Threshold -- Maximum number of BITS job interruptions	Specify the maximum number of times the BITS job can be interrupted before an event is raised. The default is 10 times.
Event severity when interruptions exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of times the BITS job is interrupted exceeds the threshold. The default is 8 (red event indicator).

BITSServiceDown

Use this Knowledge Script to monitor the status of the BITS service. This script raises an event if the service is down, and can restart the service when it is not running.

Resource Objects

BITS service object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if BITS service is down?	Set to **y** to raise an event when the BITS service is down. The default is y.
Collect data for BITS service status?	Set to **y** to collect data for charts and reports. If enabled, data collection returns a value of 100 if the service is running, and a value of 0 if the service is not running. The default is n.
Auto-start service?	Set to **y** to automatically restart the service when it is down. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager cannot restart it. The default is 5 (red event indicator).
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service was down and AppManager successfully restarted it. The default is 25 (blue event indicator).
Event severity when service down and auto-start disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager has been set to not restart the service. The default is 18 (yellow event indicator).

CLRConnectionPools

Use this Knowledge Script to monitor SQL connection pools in managed .NET applications. Connection pools are caches of stored database connections that are reused, eliminating the need to create new connections each time a new request is received.

This script raises an event if either of the following conditions exists:

- The highest number of pooled connections in a session exceeds a specified threshold.
- The total number of connection attempts that failed exceeds a specified threshold.

Note
The monitored .NET applications must be running at the time of discovery so their resource objects can be discovered. The applications must also be running for this script to collect data.

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Resource Objects

SQL Client Managed Applications folder

SQL Client Managed Applications object

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if the managed application is not running?	Set to **Yes** to raise an event if the managed application is not running. The default is Yes.
Event severity when application is not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the managed application is not running. The default is 20 (yellow event indicator).
Monitor Peak Pooled Connection	
Event Notification	
Raise event if peak pooled connections exceed threshold?	Set to **Yes** to raise an event if the number of pooled connections exceeds the threshold you set. The default is Yes.
Threshold -- Maximum peak pooled connections	Specify the maximum number of pooled connections that can occur before an event is raised. The default is 64 connections.
Event severity when peak pooled connections exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of pooled connections exceeds the threshold. The default is 15 (yellow event indicator).
Data Collection	
Collect data for peak pool connection?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the maximum number of pool connections that occurred during the monitoring interval. The default is unselected.

Parameter	How to Set It
Monitor Failed Connection	
Event Notification	
Raise event if failed connections exceed threshold?	Set to **Yes** to raise an event if the number of failed connections exceeds the threshold you set. The default is Yes.
Threshold -- Maximum failed connections	Specify the maximum of connections that can fail before an event is raised. The default is 4 connections.
Event severity when failed connections exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of failed connections exceeds the threshold. The default is 15 (yellow event indicator).
Data Collection	
Collect data for failed connections?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of connections that failed during the monitoring interval. The default is unselected.
Monitor General Connection Pool	
Data Collection	
Collect data for current connection pool?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of current connection pools. The default is unselected.
Collect data for pooled connections?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of pooled connections. The default is unselected.

CLRContention

Use this Knowledge Script to monitor the thread contention rate and thread queue length in managed .NET applications.

This script raises an event if one of the following conditions exists:

- The contention rate (in seconds) exceeds a specified threshold. Contention occurs when numerous threads compete unsuccessfully to acquire managed locks at run time.
- The thread queue length exceeds a specified threshold. Thread queue length is a measurement of all threads that are waiting to acquire a managed lock on an application.

Note
The monitored .NET applications must be running at the time of discovery so their resource objects can discovered. The applications must also be running for this script to collect data.

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Resource Objects

Managed Applications folder

Managed Applications object

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if application not running?	Set to **Yes** to raise an event if the managed application is not running. The default is Yes.
Event severity when application not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the managed application is not running. The default is 20 (yellow event indicator).
Monitor Contention Rate	
Event Notification	
Raise event if contention rate exceeds threshold?	Set to **Yes** to raise an event if the contention rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum contention rate	Specify the maximum number of contentions that can occur per second before an event is raised. The default is one contention per second.
Event severity when contention rate exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the contention rate exceeds the threshold. The default is 15 (yellow event indicator).
Data Collection	
Collect data for contention rate?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the contention rate for the monitoring interval. The default is unselected.

Parameter	How to Set It
Monitor Thread Queue Length	
Event Notification	
Raise event if thread queue length exceeds threshold?	Set to **Yes** to raise an event if the thread queue length exceeds the threshold you set. The default is Yes.
Threshold -- Maximum thread queue length	Specify the maximum number of threads that can be in the queue before an event is raised. The default is 10 threads.
Event severity when thread queue length exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of threads in the queue exceeds the threshold. The default is 15 (yellow event indicator).
Data Collection	
Collect data for thread queue length?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of threads in queue during the monitoring interval. The default is unselected.

CLRExceptions

Use this Knowledge Script to monitor exceptions that managed .NET applications raise. Exceptions are errors in a program that cause it to branch to a new routine.

This script raises an event if one of the following conditions occurs:

- The total number of .NET exceptions (or converted exceptions) that occur since the application started exceeds a specified threshold.
- The number of .NET exceptions (or converted exceptions) that occur per second exceeds a specified threshold.

Note
The monitored .NET applications must be running at the time of discovery so their resource objects can discovered. The applications must also be running for this script to collect data.

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Resource Objects

Managed Applications folder

Managed Applications object

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if application not running?	Set to **Yes** to raise an event if the managed application is not running. The default is Yes.
Event severity when application not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the managed application is not running. The default is 20 (yellow event indicator).
Monitor Exception Count	
Event Notification	
Raise event if exceptions exceed threshold?	Set to **Yes** to raise an event if the number of exceptions exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of exceptions	Specify the maximum number of exceptions that can occur before an event is raised. The default is 5 exceptions.
Event severity when exceptions exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of exceptions exceeds the threshold. The default is 15 (yellow event indicator).
Data Collection	
Collect data for number of exceptions?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of exceptions that occurred during the monitoring period. The default is unselected.

Parameter	How to Set It
Monitor Exception Rate	
Event Notification	
Raise event if exception rate exceeds threshold?	Set to **Yes** to raise an event if the exception rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum exception rate	Specify the maximum number exceptions allowed per second before an event is raised. The default is 10 exceptions per second.
Event severity when exception rate exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the exception rate exceeds the threshold. The default is 15 (yellow event indicator).
Data Collection	
Collect data for exception rate?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the exception rate during the monitoring interval. The default is unselected.

CLRHeap

Use this Knowledge Script to monitor heap memory use in managed .NET applications.

This script raises an event if one of the following occurs:

- Full garbage collection levels have changed. Total garbage collection frees memory slots in sections of unused memory and is composed of partial garbage collection (where memory freeing processes can be interrupted) and full garbage collection (where memory freeing processes cannot be interrupted). In partial garbage collection, only the most recently allocated objects (Gen 0 objects) are counted. In full garbage collection, older objects (Gen 1 and up) are counted.
- Special heap memory use is greater than a specified percentage of the total garbage collection heap. In some cases, garbage collection software allocates large objects (>20 KB) directly to an area in memory known as the special heap, bypassing generation object promotion.

Note
The monitored .NET applications must be running at the time of discovery so their resource objects can discovered. The applications must also be running for this script to collect data.

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Resource Objects

Managed Applications folder

Managed Applications object

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if application not running?	Set to **Yes** to raise an event if the managed application is not running. The default is Yes.
Event severity when application not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the managed application is not running. The default is 20 (yellow event indicator).
Monitor heap memory usage	
Event Notification	
Raise event if special heap size exceeds threshold?	Set to **Yes** to raise an event if the special heap size exceeds the threshold you set. The default is Yes.
Threshold -- Maximum size of special heap (as % of garbage heap)	Specify the maximum size of the special heap (as a percentage of the total heap) that can occur before an event is raised. The default is 80%. Total heap is the number of bytes in all heaps.
Event severity when size of special heap exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the size of the special heap exceeds the threshold. The default is 15 (yellow event indicator).

Parameter	How to Set It
Data Collection	
Collect data for total heap size?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the size of the total heap during the monitoring interval. The default is unselected.
Monitor Full Garbage Collection	
Event Notification	
Raise event if frequency of full garbage collection changes?	Set to **Yes** to raise an event if the number of full garbage collections has changed since the last time the script ran. The default is Yes.
Event severity when full garbage collection frequency changes	Set the event an event in which the number of full garbage collections has changed. The default is 15 (yellow event indicator).

CLRJit

Use this Knowledge Script to monitor JIT (just-in-time) compilation in managed .NET applications.

This script raises an event if one of the following conditions exists:

- The number of bytes per second that undergo JIT compilation (JIT byte rate) is less than a specified threshold. The JIT byte rate is the difference between the last two samples divided by the number of seconds in the interval.
- The percent of time spent in JIT compilation since the application started exceeds a specified threshold.

Note
The monitored .NET applications must be running at the time of discovery so their resource objects can discovered. The applications must also be running for this script to collect data.

Default Schedule

The default schedule for this script is **Every 15 minutes**.

Resource Objects

Managed Applications folder

Managed Applications object

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if application not running?	Set to **Yes** to raise an event if the managed application is not running. The default is Yes.
Event severity when application not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the managed application is not running. The default is 20 (yellow event indicator).
Monitor JIT Byte Rate	
Event Notification	
Raise event if JIT byte rate falls below threshold?	Set to **Yes** to raise an event if the JIT byte rate falls below the threshold you set. The default is Yes.
Threshold -- Minimum JIT byte rate	Specify the minimum number of JIT bytes that must occur per second to prevent an event from being raised. The default is 512 bytes per second.
Event severity when JIT byte rate falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the JIT byte rate falls below the threshold. The default is 15 (yellow event indicator).
Data Collection	
Collect data for JIT byte rate?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the JIT byte rate for the monitoring interval. The default is unselected.

Parameter	How to Set It
Monitor Percent of Time in JIT	
Event Notification	
Raise event if percent of time spent in JIT compilation exceeds threshold?	Set to **Yes** to raise an event if the amount of time the application spends in JIT compilation exceeds the threshold you set. The default is Yes.
Threshold -- Maximum percent of time spent in JIT compilation	Specify the maximum percentage of time the application can spend in JIT compilation before an event is raised. The default is 60%.
Event severity when time spent in JIT compilation exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of time the application spends in JIT compilation exceeds the threshold. The default is 15 (yellow event indicator).
Data Collection	
Collect data for percent of time in JIT compilation?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the amount of time the application spends in JIT compilation during the monitoring interval. The default is unselected.

CLRMemProfile

Use this Knowledge Script to monitor total garbage collection in managed .NET applications.

Total garbage collection frees memory slots in sections of unused memory and is composed of partial garbage collection (where memory freeing processes can be interrupted) and full garbage collection (where memory freeing processes cannot be interrupted).

In partial garbage collection, only the most recently allocated objects (Gen 0 objects) are counted.

In full garbage collection, older objects (Gen 1 and up) are counted.

This script raises an event if the total garbage collection time since the previous collection exceeds a specified percentage.

Note
The monitored .NET applications must be running at the time of discovery so their resource objects can discovered. The applications must also be running for this script to collect data.

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Resource Objects

Managed Applications folder

Managed Applications object

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if application not running?	Set to **Yes** to raise an event if the managed application is not running. The default is Yes.
Event severity when application not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the managed application is not running. The default is 20 (yellow event indicator).
Monitor Garbage Collection Time	
Event Notification	
Raise event if percentage of time spent in garbage collection exceeds threshold?	Set to **Yes** to raise an event if the percent of time spent in garbage collection exceeds the threshold you set. The default is Yes.
Threshold -- Maximum percentage of time spent in garbage collection	Specify the maximum amount of time the application should spend in garbage collection before an event is raised. The default is 6%.
Event severity when garbage collection time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the percent of time spent in garbage collection exceeds the threshold. The default is 15 (yellow event indicator).
Data Collection	

Parameter	How to Set It
Collect data for memory profile?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the amount of time spent in garbage collection during the monitoring interval. The default unselected.

CLRNetworking

Use this Knowledge Script to monitor network activity in managed .NET applications.

This script raises an event if one of the following conditions exists:

- The number of bytes sent during a process, through all socket connections, exceeds a specified threshold. The number of bytes includes data as well as non-TCP/IP protocol information.
- The number of bytes received during a process, through all socket connections, exceeds a specified threshold. The number of bytes includes data as well as non-TCP/IP protocol information.

Note
The monitored .NET applications must be running at the time of discovery so their resource objects can discovered. The applications must also be running for this script to collect data.

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Resource Objects

Networking Managed Applications folder

Networking Managed Applications object

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if application not running?	Set to **Yes** to raise an event if the managed application is not running. The default is Yes.
Event severity when application not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the managed application is not running. The default is 20 (yellow event indicator).
Monitor Network Traffic	
Event Notification	
Raise event if network bytes sent exceed threshold?	Set to **Yes** to raise an event if the number of bytes sent during a process exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of network bytes sent	Specify the maximum number of bytes that can be sent during a process before an event is raised. The default is 1000000 bytes.
Event severity when network bytes sent exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of bytes sent during a process exceeds the threshold. The default is 15 (yellow event indicator).
Raise event if network bytes received exceed threshold?	Set to **Yes** to raise an event if the number of bytes received during a process exceeds a specified threshold. The default is Yes.
Threshold -- Maximum number of network bytes received	Specify the maximum number of bytes that can be received during a process before an event is raised. The default is 1000000 bytes.

Parameter	How to Set It
Event severity when network bytes received exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of bytes received during a process exceeds the threshold. The default is 15 (yellow event indicator).
Data Collection	
Collect data for network byte sent?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of bytes sent during the monitoring interval. The default is unselected.
Collect data for network byte received?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of bytes received during the monitoring interval. The default is unselected.

CLRRemoting

Use this Knowledge Script to monitor remote procedure call (RPC) activity in managed .NET applications. An RPC is a type of protocol that enables a software program to execute on a remote server.

This script raises an event if the number of RPC calls per second (the RPC call rate) exceeds the threshold you set. The RPC call rate is the difference between the last two samples divided by the number of seconds in the interval.

Note
The monitored .NET applications must be running at the time of discovery so their resource objects can discovered. The applications must also be running for this script to collect data.

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Resource Objects

Managed Applications folder

Managed Applications object

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if application not running?	Set to **Yes** to raise an event if the managed application is not running. The default is Yes.
Event severity when application not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the managed application is not running. The default is 20 (yellow event indicator).
Monitor Remote Procedure Call Rate	
Event Notification	
Raise event if RPC rate exceeds threshold?	Set to **Yes** to raise an event if the number of RPCs per second exceeds the threshold you set. The default is Yes.
Threshold -- Maximum RPC rate	Specify the maximum number of RPCs that can occur per second before an event is raised. The default is 32 calls per second.
Event severity when RPC rate exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of RPC calls per second exceeds the threshold. The default is 15 (yellow event indicator).
Data Collection	
Collect data for RPC rate?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the RPC rate for the monitoring interval. The default is unselected.

CLRThreads

Use this Knowledge Script to monitor thread use in managed .NET applications. This script raises an event if one of the following conditions exists:

- The total number of threads (total recognized threads) that have run at least once since the application started exceeds a specified threshold.
- The rate at which processors are assigned to alternate threads (context switch rate) exceeds a specified threshold. For example, the kernel can reassign an operation when a thread with higher priority becomes available.

Note
The monitored .NET applications must be running at the time of discovery so their resource objects can discovered. The applications must also be running for this script to collect data.

Default Schedule

The default schedule for this script is **Every 5 minutes**.

Resource Objects

Managed Applications folder

Managed Applications object

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if application not running?	Set to **Yes** to raise an event if the managed application is not running. The default is Yes.
Event severity when application not running	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the managed application is not running. The default is 20 (yellow event indicator).
Monitor Thread Count	
Event Notification	
Raise event if thread count exceeds threshold?	Set to **Yes** to raise an event if the number threads that have run at least once exceeds the threshold you set. The default is Yes.
Threshold -- Maximum thread count	Specify the maximum number of threads that can run before an event is raised. The default is 32 threads.
Event severity when thread count exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of threads exceeds the threshold. The default is 15 (yellow event indicator).
Data Collection	
Collect data for thread count?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the number of threads that ran at least once during the monitoring interval. The default is unselected.

Parameter	How to Set It
Monitor Context Switch Rate	
Event Notification	
Raise event if context switch rate exceeds threshold?	Set to **Yes** to raise an event if the switch rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum context switch rate	Specify the maximum rate at which processors can be assigned to alternate thread before an event is raised. The default is 4096 switches per second.
Event severity when context switch rate exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the switch rate exceeds the threshold. The default is 15 (yellow event indicator).
Data Collection	
Collect data for context switch rate?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the context switch rate for the monitoring interval. The default is unselected.

DCOMAppChange

Use this Knowledge Script to monitor the distributed COM (DCOM) application list. This script raises an event if an application has been added or removed (registered or unregistered) from the application list on the target computer since the last time the script was run.

Resource Objects

For AppManager version 7.x: Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, Windows 7

For AppManager version 6.x: Windows Server 2003, Windows XP Professional

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if DCOM applications added or removed?	Set to **y** to raise an event when one or more applications have been added to or removed from the DCOM application list. The default is y.
Collect data for DCOM applications added or removed?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of DCOM applications currently registered. The default is n.
Event severity when DCOM applications added or removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which applications have been added to or removed from the DCOM application list. The default is 5 (red event indicator).

FaxActivity

Use this Knowledge Script to monitor the total number of faxes, fax pages, and fax bytes sent and received. This script raises events if the number of faxes, fax pages, or fax bytes sent and received exceeds the thresholds you set.

Resource Object

Fax folder

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if number of bytes received exceeds threshold?	Set to **y** to raise an event when the number of received fax bytes exceeds the threshold you set. The default is y.
Raise event if number of bytes sent exceeds threshold?	Set to **y** to raise an event when the number of sent fax bytes exceeds the threshold you set. The default is y.
Raise event if number of faxes received exceeds threshold?	Set to **y** to raise an event when the number of received faxes exceeds the threshold you set. The default is y.
Raise event if number of faxes sent exceeds threshold?	Set to **y** to raise an event when the number of sent faxes exceeds the threshold you set. The default is y.
Raise event if number of pages received exceeds threshold?	Set to **y** to raise an event when the number of received fax pages exceeds the threshold you set. The default is y.
Raise event if number of pages sent exceeds threshold?	Set to **y** to raise an event when the number of sent fax pages exceeds the threshold you set. The default is y.
Raise event if total number of bytes sent and received exceeds threshold?	Set to **y** to raise an event when the number of total number of sent and received fax bytes exceeds the threshold you set. The default is y.
Raise event if total number of faxes sent and received exceeds threshold?	Set to **y** to raise an event when the number of total number of sent and received faxes exceeds the threshold you set. The default is y.
Raise event if total number of pages sent and received exceeds threshold?	Set to **y** to raise an event when the number of total number of sent and received fax pages exceeds the threshold you set. The default is y.
Threshold -- Maximum number of bytes received	Specify the maximum number of fax bytes that can be received before an event is raised. The default is 20000 bytes.
Threshold -- Maximum number of bytes sent	Specify the maximum number of fax bytes that can be sent before an event is raised. The default is 20000 bytes.

Parameter	How to Set It
Threshold -- Maximum number of faxes received	Specify the maximum number of fax bytes that can be received before an event is raised. The default is 20000 bytes.
Threshold -- Maximum number of faxes sent	Specify the maximum number of faxes that can be sent before an event is raised. The default is 20000 faxes.
Threshold -- Maximum number of fax pages received	Specify the maximum number of fax pages that can be received before an event is raised. The default is 20000 pages.
Threshold -- Maximum number of fax pages sent	Specify the maximum number of fax pages that can be sent before an event is raised. The default is 20000 pages.
Threshold -- Maximum total fax bytes sent and received	Specify the maximum total number of fax bytes that can be sent and received before an event is raised. The default is 20000 bytes.
Threshold -- Maximum total faxes sent and received	Specify the maximum total number of faxes that can be sent and received before an event is raised. The default is 20000 faxes.
Threshold -- Maximum total fax pages sent and received	Specify the maximum total number of fax pages that can be sent and received before an event is raised. The default is 20000 pages.
Collect data for number of bytes received?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of fax bytes received during the monitoring interval. The default is n.
Collect data for number of bytes sent?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of fax bytes sent during the monitoring interval. The default is n.
Collect data for number of faxes received?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of faxes received during the monitoring interval. The default is n.
Collect data for number of faxes sent?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of faxes sent during the monitoring interval. The default is n.
Collect data for number of pages received?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of fax pages received during the monitoring interval. The default is n.
Collect data for number of pages sent?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of fax pages sent during the monitoring interval. The default is n.
Collect data for total number of bytes?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of fax bytes sent and received during the monitoring interval. The default is n.
Collect data for total number of faxes?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of faxes sent and received during the monitoring interval. The default is n.
Collect data for total number of pages?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of fax pages sent and received during the monitoring interval. The default is n.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8 (red event indicator).

FaxEventLog

Use this Knowledge Script to periodically scan the Windows Application event log for entries created by the Microsoft Fax service that match the criteria you specify. If any events are found, AppManager raises an event, and the event detail message provides more information about the event.

In the first interval, the value you specify for the *Start with events in past N hours* parameter determines how far back in the log to check for matching entries. As the job continues to run at subsequent intervals, it checks for any new entries created since the last time the log was checked.

You can further restrict the types of log entries that generate an event in two ways:

- Use the *Monitor for events of type [...]* parameters to search only certain types of events, such as Warning events.
- Use the *Filter the [...] field for* parameters to search only for specific information, such as events associated with a specific user or computer name.

Resource Object

Fax folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if Fax service event log entries found?	Set to **y** to raise an event if the event log contains entries that match your search criteria. The default is y.
Collect data for Fax service entries?	Set to **y** to collect data for charts and reports. When enabled, data collection returns the number of log entries found, and the data point detail message returns the text of the log entries. The default is n.
Start with events in past N hours	Use this parameter to determine which part of the event log is searched the *first* time you run the job. Subsequent searches begin where the previous one finished. The following entries are valid: • **-1** to search all existing log entries during the first interval • **n** to search entries for the past *n* hours (8 for the past 8 hours, 50 for the past 50 hours, for example.) • **0** to search no previous entries (search from the current time forward) The default is 0.

Parameter	How to Set It
Monitor for events of type:	Set to **y** for each type of event you want to monitor: • Error • Warning • Information • Success Audit • Failure Audit If you disable any of these event types, that type of log entry does not raise an event, is not returned in an event detail message, and is not collected as data if you enabled *Collect data for Fax service entries?* The default is y.
Filter the [...] field for	To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log: • **Category**. Specify one or more text strings to look for in the Category field. Separate multiple strings with commas. • **Event ID**. Specify single or multiple event IDs. Separate multiple entries with commas. To specify a range of event IDs, use a hyphen. For example: `414,1028-1400,4015`. • **User**. Specify a single or multiple user names to look for. Separate multiple entries by commas. For example: `Pat,Chris,Alex`. • **Computer**. Specify a single or multiple computer names or IP addresses to look for. Separate multiple entries by commas. For example: `SHASTA,MARS`. • **Event Description**. Specify a description or keywords in the description. The string can contain spaces, underscores, and periods. Separate multiple entries with commas. For example: `no domain,critical error from the Active Directory`. The search string can contain criteria used to include entries, exclude entries, or both. • Separate the include and exclude criteria with a colon (:). For example, `zones,caching:primary or secondary`. • Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ`. • If you are specifying only include criteria, the colon is not necessary. For example, `primary DNS domain`. • If you are specifying only exclude criteria, start the search string with a colon. For example, `:online help`.
Maximum number of entries per event	Specify the maximum number of log entries to be included in each event's detail message. If this script finds more entries in the log than the specified maximum, the script will return multiple events to report the number of entries you have specified. The default is 30 entries.
Event severity when matching Fax service log entries found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the event log contains entries that match your search criteria. The default is 8 (red event indicator).

FaxServiceDown

Use this Knowledge Script to monitor the status of the Microsoft Fax service. This script raises an event if the service is down. You can set this script to automatically attempt to restart the service when it is not running.

Resource Object

Fax service object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if Fax service is down?	Set to **y** to raise an event when the Microsoft fax service is down. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns a value of 100 if the service is running, and a value of 0 if the service is not running. The default is n.
Automatically restart service if down?	Set to **y** to automatically restart the service when it is down. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager cannot restart it. The default is 5 (red event indicator).
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in the service was down and AppManager successfully restarted it. The default is 25 (blue event indicator).
Event severity when service down and auto-start disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager has been set to not restart the service. The default is 18 (yellow event indicator).

FaxTotalFailed

Use this Knowledge Script to monitor the total number of failed faxes, failed outgoing connections, and failed receptions. This script raises an event if the number of failed faxes, failed outgoing connections, or failed receptions exceeds the threshold you set.

Resource Object

Fax folder

Default Schedule

The default interval for this script is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if number of failed faxes exceeds threshold?	Set to **y** to raise an event if the number of failed faxes exceeds the threshold you set. The default is y.
Raise event if number of failed receptions exceeds threshold?	Set to **y** to raise an event if the number of failed fax receptions exceeds the threshold you set. The default is y.
Raise event if number of failed outgoing connections exceeds threshold?	Set to **y** to raise an event if the number of failed outgoing fax connections exceeds the threshold you set. The default is y.
Threshold -- Maximum number of failed faxes	Specify the maximum number of faxes that can fail to connect or be received before an event is raised. The default is 200 faxes.
Threshold -- Maximum number of failed receptions	Specify the maximum number of faxes that can fail to be received before an event is raised. The default is 20 faxes.
Threshold -- Maximum number of failed outgoing connections	Specify the maximum number of faxes that can fail to make an outgoing connection before an event is raised. The default is 20 faxes.
Collect data for number of failed faxes?	Set to y to collect data for charts and reports. When enabled, data collection returns the number of faxes that failed to connect or be received during the monitoring interval. The default is n.
Collect data for number of failed receptions?	Set to y to collect data for charts and reports. When enabled, data collection returns the number of faxes that failed to be received during the monitoring interval. The default is n.
Collect data for number of failed outgoing connections?	Set to y to collect data for charts and reports. When enabled, data collection returns the number of faxes that failed to make an outgoing connection during the monitoring interval. The default is n.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8 (red event indicator).

FaxTotalTime

Use this Knowledge Script to monitor the number of minutes the Microsoft Fax service spends receiving faxes, the number of minutes the service spends sending faxes, and the total number of minutes the service spends receiving and sending faxes. This script raises an event if any of these values exceeds the threshold you set.

Resource Object

Fax folder

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if minutes spent receiving faxes exceeds threshold?	Set to **y** to raise an event when the number of minutes the fax service spent receiving faxes exceeds the threshold you set. The default is y.
Raise event if minutes spent sending faxes exceeds threshold?	Set to **y** to raise an event when the number of minutes the fax service spent sending faxes exceeds the threshold you set. The default is y.
Raise event if total minutes spent sending and receiving faxes exceeds threshold?	Set to **y** to raise an event when the total number of minutes the fax service spent sending and receiving faxes exceeds the threshold you set. The default is y.
Threshold -- Maximum minutes spent receiving faxes	Specify the maximum number of minutes that the fax service can spend receiving faxes before an event is raised. The default is 20000 minutes.
Threshold -- Maximum minutes spent sending faxes	Specify the maximum number of minutes that the fax service can spend sending faxes before an event is raised. The default is 20000 minutes.
Threshold -- Maximum total minutes spent receiving and sending faxes	Specify the maximum number of minutes that the fax service can spend sending and receiving faxes before an event is raised. The default is 20000 minutes.
Collect data for minutes spent receiving faxes?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of minutes the fax service spent receiving faxes during the monitoring period. The default is n.
Collect data for minutes spent sending faxes?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of minutes the fax service spent sending faxes during the monitoring period. The default is n.
Collect data for total minutes spent receiving and sending faxes?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of minutes the fax service spent sending and receiving faxes during the monitoring period. The default is n.
Event severity when any threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8 (red event indicator).

OpenSystemSlots

Use this Knowledge Script to monitor the number of available system (PCI) slots. This script raises an event if the number of available system slots falls below the threshold you set.

PCI (Peripheral Component Interconnect) slots allow different types of expansion cards to be connected inside a computer to extend the computer's functionality. Examples of PCI expansion cards are network cards, graphics cards, and sound cards.

Resource Objects

For AppManager version 7.x: Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, Windows 7

For AppManager version 6.x: Windows Server 2003, Windows XP Professional

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if available system slots fall below threshold?	Set to **y** to raise an event when the number of available system slots falls below the threshold you set. The default is y.
Collect data for number of available system slots?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of system slots that were available during the monitoring period. The default is n.
Threshold -- Minimum number of available system slots	Specify minimum number of system slots that must be available to prevent an event from being raised. The default is 1 slot.
Event severity when available system slots fall below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of available system slots falls below the threshold. The default is 5 (red event indicator).

PNPDeviceChange

Use this Knowledge Script to monitor the plug-and-play device list for any device that has been added or removed since the script was last run. This script raises an event if plug-and-play devices (for example, an external modem) are added or removed.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if plug and play devices added or removed?	Set to **y** to raise an event when a plug-and-play device is added to or removed from the device list. The default is y.
Collect data for devices added or removed?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the contents of the device list. The default is n.
Event severity when devices added or removed	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a plug-and-play device is added or removed from the device list. The default is 5 (red event indicator).

PNPDeviceErrors

Use this Knowledge Script to monitor the number of plug-and-play devices that have a status of "error." This script raises an event if the number of plug-and-play devices with error status exceeds the threshold.

Resource Objects

For AppManager version 7.x: Windows 2000 Server, Windows Server 2003, Windows XP Professional, Windows Server 2008, Windows Vista, and Windows 7

For AppManager version 6.x: Windows 2000 Server, Windows Server 2003, and Windows XP Professional

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to set it
Raise event if plug and play devices with error status exceed threshold?	Set to **y** to raise an event when the number of devices with a status of "error" exceeds the threshold you set. The default is y.
Collect data for number of devices with error status?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of devices that have the status of "error." The default is n.
Threshold -- Maximum number of plug and play devices with error status	Specify the maximum number of devices that can have an "error" status before an event is raised. The default is 10 devices.
Event severity when devices with error status exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of devices with "error" status exceeds the threshold. The default is 5 (red event indicator).

PrinterStuckJobs

Use this Knowledge Script to monitor jobs that are stuck in the printer queue. This script raises an event if the number of minutes a job has remained in the printer queue exceeds the threshold you set.

Resource Objects

Printer folder

Printer object

Default Schedule

The default interval for this script is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if time in printer queue exceeds threshold?	Set to **y** to raise an event when the number of minutes a job spends in the printer queue exceeds the threshold you set. The default is y.
Collect data for time spent in printer queue?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of minutes a job spent in the printer queue. The default is n.
Threshold -- Maximum time spent in printer queue	Specify the maximum number of minutes a job can spend in the printer queue before an event is raised. The default is 5 minutes.
Event severity when time in printer queue exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of minutes a job spends in the printer queue exceeds the threshold. The default is 1 (red event indicator).

SRDiskPercent

Use this Knowledge Script to monitor the percentage of space on a disk available for the System Restore service. The System Restore service configuration for the percentage of space available (by default this value is 12%) applies to all the computer's drives. If you enter a lower value for the threshold, this script raises an event, because the percentage of disk space available for the System Restore Service, as configured, exceeds the threshold you set.

If the amount of free disk space on a system drive falls below 200 MB, or if the amount of free disk space on a non-system drive falls below 80 MB, it is advisable to configure System Restore to turn off automatically on that drive. This script also raises an event if the space available for System Restore on any system or non-system drive falls below the threshold you set.

Resource Object

System Restore folder

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if percentage of disk space exceeds threshold?	Set to **y** to raise an event when the percentage of disk space configured for System Restore exceeds the threshold. The event detail message will include the disk space available for System Restore for each individual drive. The default is y.
Raise event if space available on a drive falls below threshold?	Set to **y** to raise an event when the space available for System Restore on any system or non-system drive falls below the threshold. The default is n.
Collect data for percentage of disk space being used?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the percentage of disk space that is configured for System Restore. The default is n.
Collect data for space available on individual drive	Set to **y** to collect data for charts and reports. If enabled, data collection returns the space available for System Restore on any system or non-system drive. The default is n.
Threshold -- Maximum disk space configured for System Restore	Specify the maximum percentage of disk space that can be configured for System Restore before an event is raised. The default is 12%.
Threshold -- Minimum disk space available on system drive	Specify the minimum amount of disk space (in MB) that should be available for System Restore on a system drive to prevent an event from being raised. The default is 200 MB.
Threshold -- Minimum disk space available on non-system drive	Specify the minimum amount of disk space (in MB) that should be available for System Restore on a non-system drive to prevent an event from being raised. The default is 80 MB.
Event severity when disk space available cannot be retrieved	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of available disk space cannot be determined. The default is 8.

Parameter	How to Set It
Event severity when disk space configured for System Restore exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of configured disk space exceeds the threshold. The default is 8.
Event severity when space available on individual drive falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the amount of available disk space for an individual drive falls below the threshold. The default is 5.

SREventLog

Use this Knowledge Script to periodically scan the Windows Application event log for entries created by the System Restore service that match the criteria you specify. This script raises an event if an entry matches criteria you specify. The event detail message provides more information about the event.

In the first interval, the value you specify for the *Start with events in past N hours* parameter determines how far back in the log to check for matching entries. As the script continues to run at subsequent intervals, it checks for any new entries created since the last time the log was checked.

You can further restrict the types of log entries that generate an event in two ways:

- Use the *Monitor for events of type [...]* parameters to search only certain types of events, such as Warning events.
- Use the *Filter the [...] field for* parameters to search only for specific information, such as events associated with a specific user or computer name.

Each time this script runs, it checks the Windows Application event log for entries matching your selection criteria and raises an event if matching entries are found. The event detail message returns the text of the log entries found. When this script is set to collect data, it returns the number of log entries found, and the data point detail message returns the text of the log entries.

Resource Object

System Restore folder

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if matching log entries found?	Set to **y** to raise an event when the log contains entries that match your search criteria. The default is y.
Collect data for matching log entries found?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of log entries found. The data point detail message returns the text of the log entries. The default is n.
Start with events in past N hours	Set this parameter to determine which part of the log to search the *first* time the job runs. Subsequent searches begin where the previous one finished. The following entries are valid: • **-1** to search all existing log entries during the first interval • **n** to search entries for the past *n* hours (8 for the past 8 hours, 50 for the past 50 hours, for example.) • **0** to search no previous entries (search from the current time forward) The default is 0.

Parameter	How to Set It
Monitor for events of type:	Set to **y** for each type of event you want to monitor: • Error • Warning • Information • Success Audit • Failure Audit If you disable any of these event types, that type of log entry does not raise an event, is not returned in an event detail message, and is not collected as data if you enabled *Collect data for matching log entries found?* The default is y.
Filter the [...] field for	To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log: • **Category**. Specify one or more text strings to look for in the Category field. Separate multiple strings with commas. • **Event ID**. Specify single or multiple event IDs. Separate multiple entries with commas. To specify a range of event IDs, use a hyphen. For example: `414,1028-1400,4015`. • **User**. Specify a single or multiple user names to look for. Separate multiple entries by commas. For example: `Pat,Chris,Alex`. • **Computer**. Specify a single or multiple computer names or IP addresses to look for. Separate multiple entries by commas. For example: `SHASTA,MARS`. • **Event Description**. Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods. Separate multiple entries with commas. For example: `no domain,critical error from the Active Directory`. The search string can contain criteria used to include entries, exclude entries, or both. • Separate the include and exclude criteria with a colon (:). For example, `zones,caching:primary or secondary`. • Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ`. • If you are specifying only include criteria, the colon is not necessary. For example, `primary DNS domain`. • If you are specifying only exclude criteria, start the search string with a colon. For example, `:online help`.
Maximum number of entries per event message	Specify the maximum number of log entries to be included in each event's detail message. If this script finds more entries in the log than the specified maximum, it will return multiple events to report the number of entries you have specified. The default is 30 entries.
Event severity when matching entries found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the log contains entries that match your search criteria. The default is 8 (red event indicator).

SRLifeInterval

Use this Knowledge Script to monitor the number of days the System Restore service preserves System Restore points.

A *restore point* is a snapshot of the system provided by the System Restore service. For example, when you install an application on your computer, a restore point is created and stored in the database. If you later want to return to the registry as it was configured before you installed the new application, select the restore point in the System Restore utility that represents your system configuration prior to installation. Your system is restored to its state before the new application was installed.

This script raises an event if the number of days that restore points have been preserved exceeds the threshold.

Resource Object

System Restore folder

Default Schedule

The default interval for this script is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if restore point lifetime exceeds threshold?	Set to **y** to raise an event when the number of days a restore point has been preserved exceeds the threshold you set. The default is y.
Collect data for length of restore point lifetime?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of days a restore point has been preserved. The default is n.
Maximum number of restore points to include in event	Specify the number of restore points to display in the event detail message. A full list of restore points can be viewed at `$(INSTALLPATH)\LifeSrPtsLog`. Restore points are displayed in order of creation date, the most recent first. The default is 20 restore points. Set to 0 to display all restore points in the event detail message.
Threshold -- Maximum restore point lifetime	Specify the maximum number of days restore points can be preserved before an event is raised. The default is 4 days.
Event severity when restore point lifetime exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of days restore points are preserved exceeds the threshold. The default is 8 (red event indicator).

SRPoints

Use this Knowledge Script to monitor the number of System Restore points that are being preserved by the System Restore service. This script raises an event if the number of System Restore points exceeds the threshold. If the System Restore system preserves too many restore points, including many old restore points, the life interval of the restore points may be too long.

Resource Object

System Restore folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if number of restore points exceeds threshold?	Set to **y** to raise an event when the number of restore points exceeds the threshold. The default is y.
Collect data for number of restore points?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of restore points being preserved by the System Restore service. The default is n.
Threshold -- Maximum total system restore points	Specify the maximum number of restore points that can be preserved before an event is raised. The default is 4 restore points.
Maximum number of restore points to include in event	Specify the number of restore points to display in the event detail message. A full list of restore points can be viewed at `$(INSTALLPATH)\ShortSrPtslog`. Restore points are displayed in order of creation date, the most recent first. The default is 20 restore points. Set to 0 to display all restore points in the event detail message.
Event severity when total number of restore points exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of preserved restore points exceeds the threshold. The default is 8 (red event indicator).

SRScheduledInterval

Use this Knowledge Script to monitor the interval, in hours, at which scheduled System Restore points are created during both current and global sessions. This script raises an event if the interval exceeds the threshold.

Exceeding the threshold means that System Restore points are being created less often than the threshold, not more often. For example, there may be five hours between System Restore points, rather than four (the default maximum threshold).

Resource Object

System Restore folder

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if global time interval exceeds threshold?	Set to **y** to raise an event when the interval at which restore points are created exceeds the time interval for global sessions. The default is y.
Raise event if current session time interval exceeds threshold?	Set to **y** to raise an event when the interval at which restore points are created exceeds the time interval for current sessions. The default is y.
Collect data for global time interval?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the restore point creation interval for global sessions. The default is n.
Collect data for current session time interval?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the restore point creation interval for current sessions. The default is n.
Threshold - Maximum global time interval	Specify the maximum interval at which restore points can be created for a global session before an event is raised. The default is every 4 hours.
Threshold - Maximum current session time interval	Specify the maximum interval at which restore points can be created for a current session before an event is raised. The default is every 4 hours.
Maximum number of restore points to include in event	Specify the number of restore points to display in the detail message.These restore points will have the description "System Check Point." A full list of restore points can be viewed at `$(INSTALLPATH)]\SysChkLog`. Restore points are displayed in order of creation date, the most recent first. The default is 20 restore points. Set to 0 to display all restore points in the event detail message.
Event severity when global time interval exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the restore point creation interval for global sessions exceeds the threshold. The default is 8 (red event indicator).
Event severity when current session time interval exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the restore point creation interval for current sessions exceeds the threshold. The default is 8 (red event indicator).

SRServiceDown

Use this Knowledge Script to monitor the status of the System Restore service. This script raises an event if the service is down. You can set this script to automatically attempt to restart the service when it is not running.

Resource Object

System Restore Service object

Default Schedule

The default interval for this script is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if System Restore service is down?	Set to **y** to raise an event when the System Restore service is down. The default is y.
Collect data for System Restore service status?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • 100 -- service is running, or • 0 -- service is not running. The default is n.
Auto-start service if down?	Set to **y** to automatically restart the service when it is down. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager cannot restart it. The default is 5 (red event indicator).
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service was down and AppManager successfully restarted it. The default is 25 (blue event indicator).
Event severity when service down and auto-start disabled	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the service is down and AppManager has been set to not restart the service. The default is 18 (yellow event indicator).

Chapter 77
Windows-RT Knowledge Scripts

The Windows-RT category provides the following Knowledge Scripts you can use with AppManager ResponseTime for Windows. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press F1.

Knowledge Script	What It Does
ChangeLocking	Lets you turn on or off the locking of a workstation so you can control access to that workstation.
ClosePlayer	Lets you shut down the Player that runs a script made by the Windows-RT Designer, such as when a running script is not working properly or a process is looping incorrectly.
TakeDesktopOwnership	Updates the Registry key indicating ownership of the desktop so that Windows-RT can run on the specified computer.

ChangeLocking

The ChangeLocking Knowledge Script allows you to turn on or off the locking of the keyboard and mouse used by a computer during the playback of a script. By default, when the Player executes a Windows-RT script on a system, Windows-RT locks all input from the mouse and keyboard for that system.

You can also change the default setting for the `InputLockOnStartup` setting in the `NetIQ.AppMan.WinRT7.Player.exe.config` file, located in the `NetIQ\AppManager\bin\Win-RT7\Player` directory.

Resource Object

WinRT7 Folder

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Enable the ability to lock mouse and keyboard input?	Select this check box to prevent input from the mouse and keyboard of the specified computer during script playback.
Raise event if the locking of the mouse and keyboard input has been successful?	Select this check box to raise an event when the input locking has been successful. The default is selected.
Event severity when the locking of the mouse and keyboard inputs has been completed successfully	Specify a severity level, from 1 to 40, to indicate the importance of the event related to discovery. Default is 35.

ClosePlayer

The ClosePlayer Knowledge Script lets you shut down the Player that runs a script made by the Windows-RT Designer.

Resource Object

WinRT

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Raise event if player closed successfully?	Select this check box to raise an event when the script player closes successfully. The default is selected.
Event severity when player closed successfully	Specify a severity level, from 1 to 40, to indicate the importance of the event in which the script player closes. The default is 35.

TakeDesktopOwnership

Use this Knowledge Script to check and update the shared Registry value used to indicate which ResponseTime module is permitted to run its associated Knowledge Scripts.

This script attempts to update the `Desktop` Registry value (located under the `HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\Response Time` Registry key) to indicate that Windows-RT Knowledge Scripts are allowed to run.

Important Because this script does not contain an embedded Windows-RT script, you cannot modify it using the Windows-RT Designer.

Resource Object

WinRT

Default Schedule

By default, this script runs once.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How To Set It
General Settings	
Job Failure Notification	
Event severity when take desktop ownership fails?	Set the event severity level, from 1 to 40, to indicate the importance of an event in which an error prevents the script from setting the Registry value to indicate that Windows-RT has ownership of the desktop. The default is 5 (red event indicator).
Raise event if take desktop ownership successful?	Select **Yes** to raise an event when the script updates the Registry value to indicate that Windows-RT has ownership of the desktop. The default is unselected.
Event severity when take desktop ownership successful?	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the script updates the Registry value indicating Windows-RT has ownership of the desktop. The default is 35.

Chapter 78
WMI Knowledge Scripts

The WMI category provides the following Knowledge Scripts for monitoring Microsoft Windows Management Instrumentation (WMI) services and executing WMI queries.

From the Knowledge Script view of the Control Center, you can access more information about any Knowledge Script by selecting it and pressing **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1.**

Knowledge Script	What It Does
Configure	Configures the frequency of the WMI repository backup and the type, size, and location of the logging files.
EventConsumer	Monitors for events generated by the WMI event provider and allows you to search for events in the database.
LogSizes	Monitors the size of WMI log files.
RepositoryUsage	Monitors the size of the WMI repository.
ResourceHigh	Monitors the CPU and memory consumption for WMI processes.
RunWQL	Allows you to run WQL statements.
ServiceDown	Monitors the availability of the WMI CIMOM service.
UserManager	Allows you to add, delete, or edit a WMI user account or WMI group account for the WMI service.
Discovery_WMI	Discovers Microsoft Windows Management Instrumentation (WMI) server configuration and resources.

Configure

Use this Knowledge Script to configure the frequency of the WMI repository backup and the type, size, and location of the logging files.

Resource Object

WMI server

Note
This Knowledge Script is not supported for WMI servers running Windows Server 2008, Windows Vista, or Windows 7.

Default Schedule

The default schedule for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if operation succeeds?	Set to **y** to raise an event when the selected operation succeeds. The default is **y**. **Note** This script always raises an event if a selected operation fails.
Time between repository backup attempts	Enter the number of minutes between WMI backup repository attempts. The default is 60 minutes.
Logging type: disable(d)/error(e)/ verbose(v)	Specify the type of log files you want created by the WMI repository backup operation. Valid values are: • **d** to disable logging (no log file is created) • **e** to enable error logging (log file records any errors encountered) • **v** to enable verbose logging (log file includes error and informational messages) The default is **e**.
Maximum log file size	Enter the maximum size of the log file in bytes. If the log file exceeds this size, the file is truncated. The default is 65535 bytes.
Logging directory	Enter the name of the directory to use for log files.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...configuration succeeded**. The default is 25 (blue event indicator). • **...configuration failed**. The default is 5 (red event indicator).

EventConsumer

Use this Knowledge Script to search a specific WMI repository namespace for events generated by the event provider. Enter the search criteria using the Windows Management Instrumentation Query Language (WQL). You can perform event queries with this script using the `SELECT` statement and related `WITHIN`, `GROUP`, and `HAVING` clauses. For more information about WQL, refer to the Microsoft documentation.

This script raises an event when events matching your query are found in the WMI repository. You specify the WMI event properties to display in the AppManager event.

Resource Object

WMI server

Default Schedule

The default schedule for this script is **Asynchronous**. This script will run indefinitely until you stop the script.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Path to the WMI namespace	Specify the path to the WMI namespace you want to monitor. The default is `root\cimv2`.
WMI event query	Specify the information you want to find in the WMI repository using the WQL query format. The default query is: `select * from __InstanceCreationEvent within 1 where TargetInstance is a 'Win32_NTLogEvent'`
Fields to display for the event in the List pane	Specify the type of event information to display in the Message field in the List pane of the Operator Console. By default, the Source Name and Event ID fields are displayed. For example, if the source of an event is `MSSQLSERVER` and the Event ID is `17055`, the information displayed in the Message field would be `MSSQLSERVER - 17055`. **Note** This parameter requires case-sensitive entries. For example, do not enter `sourcename` if the actual field name is `SourceName`.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

LogSizes

Use this Knowledge Script to monitor the size of the following WMI log files:

- cimom.log
- mofcomp.log
- wbemcore.log
- wbemprox.log

This Knowledge Script allows you to set a maximum log file size for individual log files and a maximum size for the sum of all log files. If either threshold is exceeded, an event is raised.

Note
This Knowledge Script is not supported on the Microsoft Windows Vista, or later, operating system.

Resource Object

WMI Log file object

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data for all log files?	Set to **y** to collect data for all log files. If set to **y**, the script returns the total file size used by all log files. The default is **n**.
Collect data for individual log files?	Set to **y** to collect data for individual log files. If set to **y**, the script returns the file size used by each log file. The default is **n**.
All log files size maximum threshold	Enter a threshold in MB for the maximum total file size used by all log files. The default is 1000 MB.
Individual log files size maximum threshold	Enter a threshold in MB for the maximum size of each log file. The default is 50 MB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

RepositoryUsage

Use this Knowledge Script to monitor the size of the WMI repository. If the repository size exceeds the threshold you set, an event is raised.

Resource Object

WMI Repository folder

Default Schedule

The default interval for this script is **Once every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for graphs and reports. If set to **y**, the script returns the size of the WMI repository in MB. The default is **n**.
Repository size	Enter a threshold in MB for the repository size. The default is 500 MB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

ResourceHigh

Use this Knowledge Script to monitor CPU and memory consumption by the WMI service (`Winmgmt`). This script raises an event if CPU usage or memory usage exceeds the threshold you set.

Note

Beginning with Microsoft Windows XP, the `Winmgmt` service runs with several other services under an instance of the `svchost.exe` process. Therefore, when the ResourceHigh Knowledge Script monitors CPU and memory for the `Winmgmt` service, it is actually monitoring these same metrics for all services hosted by the instance of the `svchost.exe` process.

If you set the *Collect data?* parameter to **y**, the values returned for percentage of CPU used and MB of memory used are sums of CPU usage and memory usage for all services hosted by the `svchost.exe` process. The values do not represent CPU and memory usage for only the `Winmgmt` service.

Resource Object

WMI server

Default Schedule

The default interval for this script is **Every 10 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for graphs and reports. If set to **y**, the script returns the percentage of CPU resources and the MB of memory used by the WMI service. The default is **n**.
% CPU maximum threshold	Enter a threshold for the maximum percentage of CPU resources that WMI should be allowed to consume. The default is 60%.
Memory maximum threshold (in MB)	Enter a threshold in MB for the maximum amount of memory WMI should be allowed to consume. The default is 6 MB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8 (red event indicator).

RunWQL

Use this Knowledge Script to run WQL queries. You can enter the WQL query to be executed as a parameter of this Knowledge Script, or you can load the query from a script file. You can choose the data output to be a specified number of data rows (all columns) or the value of the first row of a specific column (the column is specified by either number or name).

Examples of simple WQL queries:

```
/* Command to get the path setting for a computer. */
Select * from Environment where Name = 'Path'

/* Command to get information about the provider CIMWin32. */
Select * from _Win32Provider where Name = 'CIMWin32'
```

Resource Object

WMI server

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise events. The default is **y**.
Collect data?	Set to **y** to collect data for graphs and reports. The default is **y**.
WQL query	Enter the WQL query that will run. The default query is: `SELECT Caption, ThreadCount FROM win32_Process` **Tip** Unless you are entering very simple queries, you may find that typing WQL statements in this field is error-prone. To avoid errors, you can use the *Load WQL script from file* parameter. Alternatively, if you have an AppManager Developer's license, you can check this Knowledge Script out of the repository, use the Knowledge Script Editor to paste the desired WQL statements into the WQL query field, and then check in the modified Knowledge Script.
Load WQL script from file?	Set to **y** to load an existing WQL script. The file containing the script must be present on the computer on which the Knowledge Script job will run. The default is **n**.
WQL script file (full path)	Enter the full path to the file that contains the WQL script (for example: `C:\netiq\Sample.wql`). **Note** This path is relative to the computer on which the Knowledge Script job will run.
WMI server\namespace	Enter the name of the managed WMI server and CIM namespace. The default is `root\CIMv2`.

Description	How to Set It
Return N rows (set to 0 for all rows)	Enter the number of rows to return as data output when the *Collect data?* parameter is set to **y**. The default is 10. **Note** You can set this value to 0 to set no limit on the number of rows returned. However, there is a limit of 32K for the total of returned data.
Return first row of specified column?	Set to **y** to use a specified column number or column name from which data will be returned (specify the column number or name in one of the two following parameters). Setting this parameter to **y** will override the *Return N rows* parameter. The default is **n**.
Column number	If the *Return first row of specified column?* parameter is set to **y**, the value of the first row of the column specified here (by number), rather than the number of rows, is used as data output. The default is 0.
Column name	If the *Return first row of specified column?* parameter is set to **y**, the value of the first row of the column specified here (by name), rather than the number of rows, is used as data output. The default is blank.
GivenLegend	String used in the Legend column of graph data. If this value is left blank, the Legend column will read: “WQL query results on WMI Server: <machine name>.”
Maximum threshold	Set the high watermark for the return value of the WQL query (this value can be the number of rows returned or the value of the first row of a specified column, depending on the type of data output you chose). If the return value exceeds this limit, an event will be raised. The default is 10000.
Minimum threshold	Set a low watermark for the return value of the WQL query (this value can be the number of rows returned or the value of the first row of a specified column, depending on the type of data output you chose). If the return value is below this limit, an event will be raised. The default is 10.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5 (red event indicator).

ServiceDown

Use this Knowledge Script to monitor the WMI CIMOM (Common Information Model Object Manager) service. If the CIMOM service is not running, an event is raised. Optionally, you can set the Knowledge Script to attempt to restart the service automatically.

Resource Object

WMI service object

Default Schedule

The default interval for this script is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Set to **y** to collect data for graphs and reports. The default is **n**. If set to **y**, the script returns a value of 100 if the CIMOM service is running and a value of 0 if the service is not running.
Auto-start service?	Set to **y** to automatically restart down services. The default is **y**.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: • **...service down; restart failed**. The default is 5 (red event indicator). • **...service down; restart succeeded**. The default is 25 (blue event indicator). • **...service down; don't restart**. The default is 18 (yellow event indicator).

UserManager

Use this Knowledge Script to add, delete, or edit WMI user or group accounts for the WMI service on the computer where the Knowledge Script job is running. You can also use this Knowledge Script to manage user access to CIM objects.

This script can add or modify domain accounts or groups. The account or group you are modifying must belong to the same domain as the computer on which the script is running.

By default, this script raises an event whose message informs you of the success or failure of the operation.

If you want to use this script to manage an account that was added from the WMI Control, that account must meet the following requirements:

- Permissions must be granted for **This namespace and subnamespaces**.
- Permissions must allow Provider Write, Enable Account, and Remote Enable.

Resource Object

WMI server

Note
This Knowledge Script is not supported for WMI servers running Windows Server 2008, Windows Vista, or Windows 7.

Default Schedule

The default interval for this script is **Run once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if operation succeeds?	Set to **y** to raise an event when the selected operation succeeds. The default is **y**. **Note** This script always raises an event if a selected operation fails.
Manage user or group?	Set to **u** to manage user accounts. Set to **g** to manage group accounts. The default is **u**.
Operation to perform: add(a)/ delete(d)/edit(e)	Indicate the type of operation you want to perform. Set to one of the following: • **a** to Add users or groups • **d** to Delete users or groups • **e** to Edit users or groups The default is **a**.
User or Group names to be managed	Enter the user or group account name you want to manage. You can enter multiple names, separated by commas with no spaces. For example: `guest,admin,user1` The default is guest.
Domain name	Enter the domain name associated with the user or group account. You must specify the local machine name when deleting or editing a local user.

Description	How to Set It
Enable this account?	Set to **y** to enable the specified accounts if you are adding new user or group accounts or editing existing accounts. Set to **n** to disable an account. The default is **y**.
Can this account execute methods?	Set to **y** to give the specified accounts permission to execute methods exported from the CIM Object Manager. The default is **n**.
Schema access privileges: Read-only(r) / Write instance(i) / Write class(c)?	Indicate the WMI schema access allowed for the specified accounts. Set to: • **r** to authorize read-only access (users can execute queries or retrieve instances and classes, but cannot create, delete, or modify CIM objects). • **i** to allow the account read/write/delete access to instances in the WMI schema and read-only access to classes. • **c** to allow the account full read/write/delete access to all CIM objects, classes, and instances in the WMI schema. The default is **r**.
Can this account edit security?	Set to **y** to give the specified accounts permission to edit security. When set to **y**, the user has read and write access to the ROOT\Security namespace. When set to **n**, the user cannot access the ROOT\Security namespace. The default is **n**.
Group account type: NTLM Local(l)/NTLM Global(g)	Indicate whether the specified group accounts are local to the managed computer or global. Set to: • **l** to create a local Windows group (that can only access the local workstation or domain). • **g** to create a domain global group (that can access its own domain, member servers and workstations in the domain, and trusting domains). This parameter is used only for managing group accounts. The default is **l**.
Event severity level	Set the severity level, from 1 to 40, to indicate the importance of the event. The default is 12 (yellow event indicator).

Discovery_WMI

Use this Knowledge Script to discover the Microsoft Windows Management Instrumentation (WMI) server configuration and resources.

Resource Object

WMI server

Default Schedule

By default, this script is only run **once** for each computer.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: • **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). • **...fails**. The default is 5 (red event indicator). • **...is not applicable**. This type of failure usually occurs when the target computer does not have WMI installed. The default is 15 (yellow event indicator).

Chapter 79
WTS Knowledge Scripts

The WTS category provides the following Knowledge Scripts for monitoring Microsoft Windows Terminal Server resources.

From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
LoggedOffSessions	Collects data about completed sessions hosted by Terminal Server.
Messenger	Sends a message to a user currently connected to a Windows Terminal Server session.
SessionsInfo	Reports information about the current terminal sessions connected to the Windows Terminal Server.
SessionsLogoff	Terminates a Windows Terminal Server session.
SessionsReset	Resets a client session on a Windows Terminal Server.
SessionsTimeout	Monitors the current number of sessions timed out.
SessionsTotalActive	Monitors the current number of active client sessions. Active sessions are sessions currently logged on to the Windows Terminal Server.
SessionsTotalBytes	Monitors the total number of input and output bytes used in a session.
SessionsTotalDisconnected	Monitors the total number of sessions disconnected on a Windows Terminal Server.
SessionsTotalErrors	Monitors the total number of session errors.
SessionsTotalFrames	Monitors the total number of frames or packets transmitted in a session.
SessionsTotalInactive	Monitors the number of inactive Windows Terminal Server sessions.
SessionsTotalProtocolHitRatio	Monitors the overall hit ratio for all protocol objects per session.
TopCpuProcs	Monitors CPU usage for all WTS processes and the CPU used by each of the top *n* number of processes.
TopCPUSessions	Monitors CPU usage for all WTS sessions and the CPU usage used by each of the top n number of sessions. Runs only on Windows 2000 or later.

Knowledge Script	What It Does
TopMemorySessions	Monitors total memory usage for all sessions and the memory used by each of the top *n* number of sessions. Runs only on Windows 2000 or later.
UsersInfo	Displays information about the users currently logged on to the Windows Terminal Server.

LoggedOffSessions

Use this Knowledge Script to collect data about the completed sessions hosted by Windows Terminal Server.

This Knowledge Script scans all user sessions and makes a note of a user's name, session ID, and logon time. On subsequent scans, it compares the current user sessions with its notes from previous sessions. For each user that is no longer logged on, the Knowledge Script returns the user name, the session ID, the logon time, and the current time that is, the time when the Knowledge Script ran and detected that the session has ended. The script also calculates a maximum session duration by subtracting the logon time from the current time.

You can also set a threshold for the maximum number of sessions that can end in any interval.

The accuracy of the data returned by this Knowledge Script improves depending on how frequently you set it to run:

- The Knowledge Script cannot detect sessions that start and end between the intervals when it runs. For example, let us say you schedule the script to run every hour on the hour. A session that starts at 10:15 and ends at 10:45 will not be detected by the script when it runs at 10:00 and 11:00.
- The maximum duration is calculated using the time when the script runs and notices that a previous session is no longer active. If, for example, the script runs at 30-minute intervals and a session ends 1 minute after the script runs, 29 minutes elapse until the next time the script runs, and the maximum duration is 29 minutes longer than the actual session time.

In both cases, the accuracy of the data returned improves substantially when you schedule to run at, for example, every minute.

Resource Object

Windows Terminal server

Default Schedule

The default schedule is **Every hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event when threshold is exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data for completed user sessions? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, this script returns the user name, the session ID, the logon time, the current time that is, the time when the Knowledge Script ran and detected that the session ended, and the maximum session duration, which is the current time minus the logon time. The default is y.
Threshold--completed user sessions	Enter the maximum number of user sessions that can end in any given interval before an event is raised. The default is 0.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 8 (red event indicator).

Example of How This Script is Used

One common use of this Knowledge Script is to provide billing information for the use of WTS services. Each data point returned by the Knowledge Script represents a complete, billable session. When using this Knowledge Script for this purpose, remember that the accuracy of the "maximum duration" returned by this script depends on how frequently you run the Knowledge Script.

Messenger

Use this Knowledge Script to send a message to a user currently connected to a Windows Terminal Server session.

You can specify the recipients for the message by user name, session name, session ID, or by entering a file name that contains a list of recipients by user name, session name, or session ID. User names must not include spaces. The file name must be a complete path using the '@' symbol, for example: `@c:\recipient.txt`. Enter an asterisk (*) to include all sessions.

Resource Object

Windows Terminal server

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Recipients (separate with commas)	Enter a list of recipients for the message, separated by commas with no spaces. You can specify sessions by user name, session name, session ID, or file name. Names cannot include spaces. For example: `wsmith,jcarter,001003` If you enter a file name that contains a list of recipients, enter a complete path including the "@" symbol. For example: "`@c:\recipient.txt`". **Notes** • Ensure that the list of recipients listed in the file are separated by line breaks and not special characters. • The recipient text file must contain only the list recipients currently connected to a Windows Terminal Server. Enter an asterisk (*) to send a message to all sessions.
Event if sending message fails? (y/n)	Set to **y** to raise an event if the message delivery fails. The default is y.
Collect data for messages sent? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the number of sessions that received the message. The default is n.
Delay (time to wait for the receiver to acknowledge the message)	Enter the number of seconds to wait for the recipient to acknowledge receiving the message. After the number of seconds has passed, the message automatically closes. The default is 0 seconds. The message is displayed until it is acknowledged by the user.

Description	How to Set It
Message	Enter the text of the message you want to send. **Notes** • If you want to include double quote characters in the text of your message, you must use two double quote characters before and after the word(s) you want to enclose. For example, if you want the word Server enclosed in double quotes, you should enter the string `""Server""`. Failure to follow this syntax causes an error when you run this script. • The length of the text message must not exceed 246 characters.
Event severity when message sent fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

SessionsInfo

Use this Knowledge Script to display information about the current terminal sessions connected to the Windows Terminal Server. The information returned in the detailed data message depends on the version of Windows Terminal server:

- With some versions, the data message contains the session name, user name, session ID, current status, session type, and device.
- With other versions, the data message contains the session name, user name, session ID, current status, client address, and client name.

If the Knowledge Script cannot get information about the Windows Terminal Server sessions, an event is raised.

Resource Object

WTS Sessions

Default Schedule

The default schedule is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Collect data on terminal session information? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns for current number of sessions connected to the target computer. The default is y.
Event severity if information cannot be retrieved	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 8 (red event indicator).

SessionsLogoff

Use this Knowledge Script to terminate a Windows Terminal Server session. You can specify the sessions to log off by session name or session ID. If the Knowledge Script fails, an event is raised.

Resource Object

WTS Sessions

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Session Name or Session ID	Enter a list of sessions you want to terminate, separated by commas with no spaces. You can specify sessions by session name or session ID number. For example: `RDP-TCP#8, RDP-TCP#9, 4`.
Event if sessions cannot be logged off? (y/n)	Set to **y** to raise events if the operation fails for any reason. The default is y.
Collect data for sessions logged off? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the number of sessions terminated. The default is n.
Event severity when session logoff fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

SessionsReset

Use this Knowledge Script to reset a client session on a Windows Terminal Server. When you run this Knowledge Script, the session's hardware and software subsystems are reset to known initial values. You can identify the session to reset by session name or session ID number. If the Knowledge Script fails, an event is raised.

Resource Object

WTS Sessions

Default Schedule

The default schedule is **Run once**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Session Name or Session ID	Enter a list of sessions you want to reset, separated by commas with no spaces. You can specify sessions by session name or session ID number. For example: `RDP-TCP#8, RDP-TCP#9, 4`.
Event if session reset fails? (y/n)	Set to **y** to raise events if the operation fails for any reason. The default is y.
Collect data for reset sessions (y/n)?	Set to **y** to collect data for reports and graphs. If set to y, the script returns the number of sessions reset. The default is n.
Event severity when reset fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

SessionsTimeout

Use this Knowledge Script to monitor The total number of timeouts on the communication line from both the host and client sides of the connection. These are typically the result of a noisy line. On some high latency networks, this could be the result of the protocol timeout being too short.

If the number of timed out sessions exceeds the threshold you set, an event is raised. Increasing the protocol timeout on these types of lines will improve performance by reducing needless re-transmissions.

Resource Object

WTS Sessions

Default Schedule

The default schedule is **Every 1800 seconds**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event if session timeouts exceed threshold? (y/n)	Set to **y** to raise events. The default is y.
Collect data for session timeouts? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the total number of active sessions. The default is y.
Threshold--maximum session timeouts per interval	Enter the maximum number sessions that can be timed out before raising an event. The default is 0 timed out sessions.
Event severity if session timeouts threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

SessionsTotalActive

Use this Knowledge Script to monitor the current number of active client sessions. Active sessions are sessions currently logged on to the Windows Terminal Server. If the number of active sessions exceeds the threshold you set, an event is raised.

Resource Object

WTS Sessions

Default Schedule

The default schedule is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event if threshold is exceeded?	Set to **y** to raise events. The default is y.
Collect data for active sessions? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the total number of active sessions. The default is y.
Threshold--maximum active sessions	Enter the maximum number of concurrent sessions to be active before raising an event. The default is 50 sessions.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

SessionsTotalBytes

Use this Knowledge Script to monitor the total number of input and output bytes used in a session. The total number of bytes includes memory used to handle any protocol overhead. If the number of bytes used in a session exceeds the threshold you set, an event is raised.

Resource Object

WTS Sessions

Default Schedule

The default schedule is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event if threshold exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data for total bytes per session? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the number of bytes used by each session. The default is y.
Threshold--total bytes used per session	Enter the maximum number of bytes to be used per session before an event is raised. The default is 500 bytes.
Event severity if threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

SessionsTotalDisconnected

Use this Knowledge Script to monitor the total number of sessions disconnected on a Windows Terminal Server. If the number of disconnected sessions exceeds the threshold you set, an event is raised.

Resource Object

WTS Sessions

Default Schedule

The default schedule is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event when threshold is exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data for disconnected sessions? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, this script returns total number of errors for each session. The default is n.
Threshold--maximum disconnected sessions	Enter the maximum number of sessions to be disconnected before an event is raised. The default is 10 disconnected sessions.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 8 (red event indicator).

SessionsTotalErrors

Use this Knowledge Script to monitor the total number of session errors of all types. The total number of errors for a session can include lost acknowledgments, badly formed packets, and transmission problems. If the number of errors exceeds the threshold you set, an event is raised.

Resource Object

WTS Sessions

Default Schedule

The default schedule is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event if threshold exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data for session errors?	Set to **y** to collect data for reports and graphs. If set to y, this script returns total number of errors for each session. The default is y.
Threshold--maximum session errors	Enter the maximum number of errors to occur for any session before an event is raised. The default is 500 errors.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

SessionsTotalFrames

Use this Knowledge Script to monitor the total number of frames or packets transmitted in a session. If the number of frames exceeds the threshold you set, an event is raised.

Resource Object

WTS Sessions

Default Schedule

The default schedule is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event if threshold is exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data for frames transmitted per session? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, this script returns total number of frames for each session. The default is y.
Threshold--maximum transmitted frames	Enter the maximum number of frames to be transmitted in a session before an event is raised. The default is 30 frames per session.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

SessionsTotalInactive

Use this Knowledge Script to monitor the number of inactive Windows Terminal Server sessions. If the number of inactive sessions exceeds the threshold you set, an event is raised.

Resource Object

WTS Sessions

Default Schedule

The default schedule is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event if threshold is exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data for inactive sessions? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the total number of inactive sessions. The default is y.
Threshold--maximum inactive sessions	Enter the maximum number of sessions to be inactive before an event is raised. The default is 50 inactive sessions.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

SessionsTotalProtocolHitRatio

Use this Knowledge Script to monitor the overall hit ratio for all protocol objects per session. The hit ratio is the percentage of time protocol objects that are reused or available in the client cache. A higher hit ratio indicates reduced data transmission and better performance. A low hit ratio is caused when a session is updated with new information that is not re-used, or is not used within the number of bytes available for the client cache. If the hit ratio for any session is lower than the threshold you set, an event is raised.

Resource Object

WTS Sessions

Default Schedule

The default schedule is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event if the protocol hit ratio is below threshold? (y/n)	Set to **y** to raise events. The default is y.
Collect data for protocol hit ratio? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the total number of active sessions for graphing. The default is n.
Threshold--minimum protocol hit ratio	Enter the minimum protocol hit ratio percentage per session to be reached before an event is raised. The default is 50%.
Event severity if below threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

TopCpuProcs

Use this Knowledge Script to monitor CPU usage for all WTS processes and the CPU used by each of the top *n* number of processes. If the total percentage of CPU usage for the top *n* number of processes exceeds the threshold you set, an event is raised. You can specify the number of top processes to display in the detail message. The detail message includes the percentage of CPU used by each of the top *n* number of processes.

Resource Object

WTS server

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event if threshold is exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data for CPU usage by top processes? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the total CPU usage for the top *n* number of processes. The default is n.
Threshold--maximum CPU usage	Enter the maximum percentage of CPU resources WTS processes can consume before raising an event. The default is 90%.
Number of top CPU usage processes to show	Specify the number of top processes to display in the detail message. Enter 0 if you want to display all processes. The default is 5 processes.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

TopCPUSessions

Use this Knowledge Script to monitor CPU usage for all WTS sessions and the CPU usage used by each of the top *n* number of sessions. If the total percentage of CPU usage for the top *n* number of sessions exceeds the threshold you set, an event is raised. You can specify the number of top sessions to display in the detail message. The detail message includes the percentage of CPU usage used by each of the top *n* number of session.

Resource Object

WTS sessions

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event when CPU usage exceeds threshold? (y/n)	Set to **y** to raise events. The default is y.
Collect data for session CPU usage? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the total CPU usage for the top *n* number of sessions. The default is n.
Threshold--total CPU usage	Enter a threshold for the maximum percentage of CPU resources WTS sessions can consume before raising an event. The default is 90%.
Number of top CPU usage sessions to show	Specify the number of top sessions you want to display in the detail message. Enter 0 if you want to display all sessions. The default is 5 sessions.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

TopCpuUsers

Use this Knowledge Script to monitor CPU usage for each user logged on a Windows Terminal Server. If the percentage of CPU usage for the top *n* number of users exceeds the threshold you set, an event is raised. You can specify the number of top users to display in the detail message. The detail message includes the percentage of CPU used by each of the top *n* number of users.

Note
This script is only supported on Windows NT Terminal Servers.

Resource Object

WTS Users

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event if threshold is exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data for user CPU usage? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the total CPU usage for the top *n* number of users. The default is n.
Threshold -- maximum CPU usage	Enter the maximum percentage of CPU resources the top *n* number of users can consume before raising an event. The default is 90%.
Number of top processes to show	Enter the number of top users you want to display in the detail message. Enter 0 if you want all to display all users. The default is 5 users.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

TopMemorySessions

Use this Knowledge Script to monitor total memory usage for all sessions and the memory used by each of the top *n* number of sessions. If the memory usage of any of the sessions exceeds the threshold you set, an event is raised. You can specify the number of top sessions to display in the detail message. The detail message includes the total memory used by each of the top *n* number of sessions.

Resource Object

WTS sessions

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event if threshold is exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data for session memory usage? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the total memory usage for the top *n* number of sessions. The default is n.
Threshold--maximum memory usage	Enter the maximum memory the top *n* number of sessions can consume before raising an event. The default is 5,120 KB.
Number of top usage of memory sessions to show	Enter the number of top sessions you want to display in the detail message. Enter 0 if you want all to display all users. The default is 5 memory sessions.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

TopMemoryUsers

Use this Knowledge Script to monitor total memory usage for all users and the memory used by each of the top *n* number of users logged on to a Windows Terminal Server. If the memory usage in KB of the working set for any user exceeds the threshold you set, an event is raised. You can specify the number of top users to display in the detail message. The detail message includes the total memory used by each of the top *n* number of users.

Note
This Knowledge Script is only supported on Windows NT Terminal Servers.

Resource Object

WTS Users

Default Schedule

The default schedule is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event if threshold is exceeded? (y/n)	Set to **y** to raise events. The default is y.
Collect data for user memory usage? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the total memory usage for the top *n* number of users. The default is n.
Threshold -- maximum memory usage	Enter the maximum memory the top *n* number of users can consume before raising an event. The default is 5120 KB.
Number of top memory users to show	Enter the number of top users you want to display in the detail message. Enter 0 if you want to display all users. The default is 5 users.
Event severity when threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 5 (red event indicator).

UsersInfo

Use this Knowledge Script to display information about the users currently logged on to the Windows Terminal Server. The detailed message includes each user's name, session name, session ID, current status, idle time, and log on time. If the Knowledge Script cannot get information about Windows Terminal Server users, an event is raised.

Resource Object

WTS Users

Default Schedule

The default schedule is **Every 1 hour**.

Setting Parameter Values

Set the following parameters as needed.

Description	How to Set It
Event severity if information cannot be retrieved	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 8 (red event indicator).
Collect data for logged on users? (y/n)	Set to **y** to collect data for reports and graphs. If set to y, the script returns the number of users currently connected to WTS. The default is y.

Example of the Information Returned

The following is an example of the data collected and displayed in the data detail message:

```
USERNAME    SESSIONNAME     ID  STATE  IDLE TIME  LOGON TIME
>shawn      console          0  active          .  09/03/03 18:56
 netiq                       4  disc         none  09/04/03 10:32
 netiq      rdp-tcp#5        5  active         50  09/04/03 12:05
```